Table of Content

■ **Chapter 1 Product Overview.....1**

A. Introduction.....1

B. Package Contents.....1

C. Optional.....1

■ **Chapter 2 Your First Time on Digital KVM via IP.....2**

A. Quick Start Guide.....2

B. Disabling the Mouse Acceleration on the Host computer(s) and Client Computer.....8

C. How to Connect your **Digital KVM via IP**.....9

D. Access your **Digital KVM via IP** and Remote Control the Host Computer(s).....11

■ **Chapter 3 Advanced Operations.....12**

A. How to login the **Digital KVM via IP**.....12

B. Configure your **Digital KVM via IP**.....**14**

I. How to Setup Personal Preferences..... 14

II. How to Get the Snapshots..... 16

III. How to Remote Control the Host Computer(s)..... 17

IV. How to Setup the IP Address for your **Digital KVM via IP**.....18

V. How to Edit the User Accounts.....20

VI. How to Setup your **Digital KVM via IP** System Identification.....21

VII. How to Strengthen your **Digital KVM via IP** System Security.....22

VIII. How to Setup your **Digital KVM via IP** with the External Power Bar and Keyboard Mapping 25

IX. How to Setup the SNMP Agent and Configuration.....26

X. How to Setup RADIUS authentication.....27

XI. How to Setup and Control the External Serial Consoles.....28

XII. How to Set Date and Time.....29

XIII. How to Update your Firmware.....30

XIV. How yo Upload Custom Certificate.....32

XV. How to Lookup your **Digital KVM via IP** System Status.....33

XVI. How to Setup Port Number.....34

XVII. How to Speed up your **Digital KVM via IP**.....35

■ **Chapter 4 Accessing KVM Features.....37**

A. Cascade Configuration.....37

B. KVM-OSD Operations.....38

C. Hot Key Commands.....41

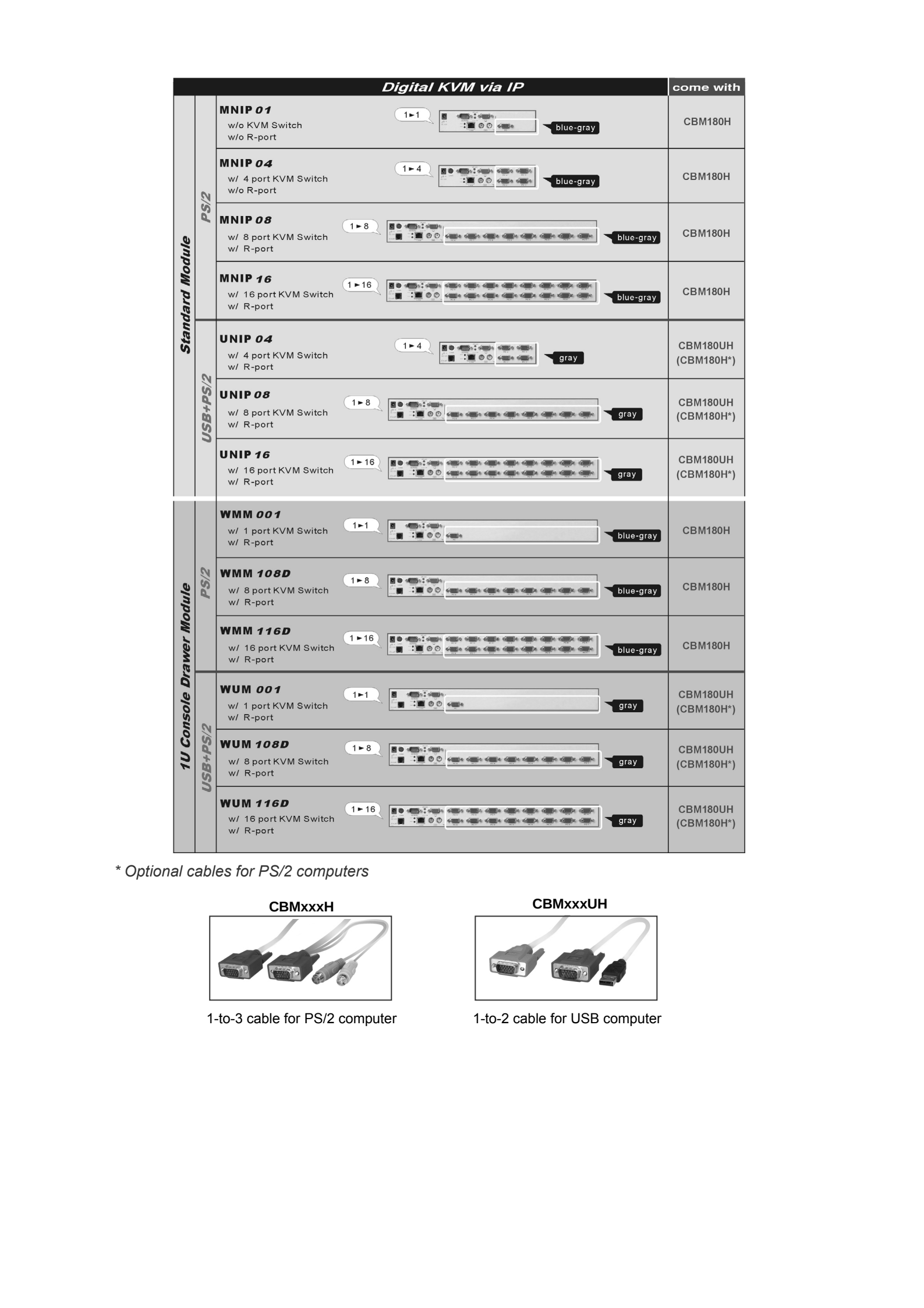
■ **Chapter 5 How to Remotely Control the Host computer(s) 43**
A. Accessing the VNC Interface 43
I. Web Interface 43
II. Native VNC Client 43
III. SSH Tunnel 43
B. Using the VNC Menu **45**
C. How to Use the Bribar 45
D. How to Use the Main Menu 47
E. How to Use the Virtkeys Menu 48
F. How to Use the Video Tuning Menu 49

Appendices

Appendix A Troubleshooting 50
Appendix B Specifications 53
Appendix C Supported Protocols 55
Appendix D Warranty Information 56
Appendix E Regulatory Compliance Statements 57
Appendix F About Security Certificate Warnings 58
Appendix G Using Optional **Serial Supervisor** Module (IPMI supported) with the **R-Port** 59
Appendix H Using Optional Modem Feature 67

NOTE: Since firmware for our **Digital KVM via IP** Products is constantly evolving to offer more functionality and improvements, some of the options and instructions presented in this manual may differ from your unit. To obtain the latest documentation and support information for our **Digital KVM via IP** products, please visit **www.rextron.com**

Digital KVM via IP			come with
Standard Module	PS/2	**MNIP *01*** w/o KVM Switch w/o R-port	CBM180H
		MNIP *04* w/ 4 port KVM Switch w/o R-port	CBM180H
		MNIP *08* w/ 8 port KVM Switch w/ R-port	CBM180H
		MNIP *16* w/ 16 port KVM Switch w/ R-port	CBM180H
	USB+PS/2	**UNIP *04*** w/ 4 port KVM Switch w/ R-port	CBM180UH (CBM180H*)
		UNIP *08* w/ 8 port KVM Switch w/ R-port	CBM180UH (CBM180H*)
		UNIP *16* w/ 16 port KVM Switch w/ R-port	CBM180UH (CBM180H*)
1U Console Drawer Module	PS/2	**WMM *001*** w/ 1 port KVM Switch w/ R-port	CBM180H
		WMM *108D* w/ 8 port KVM Switch w/ R-port	CBM180H
		WMM *116D* w/ 16 port KVM Switch w/ R-port	CBM180H
	USB+PS/2	**WUM *001*** w/ 1 port KVM Switch w/ R-port	CBM180UH (CBM180H*)
		WUM *108D* w/ 8 port KVM Switch w/ R-port	CBM180UH (CBM180H*)
		WUM *116D* w/ 16 port KVM Switch w/ R-port	CBM180UH (CBM180H*)



** Optional cables for PS/2 computers*

CBMxxxH

1-to-3 cable for PS/2 computer

CBMxxxUH

1-to-2 cable for USB computer

■ Chapter 1 Product Overview

A. Introduction

Thank you for purchasing **Rextron Digital KVM via IP** series with integrated KVM. Using the Internet or your TCP/IP enabled network, you can now remotely monitor and control critical PC servers and workstations using an industry-standard Web browser or VNC client.

- **RoHs compliant**
- **16 bits color depth supports up 65,536 colors**
- **Unique OSD feature to guide the user finish the initial setup step-by-step very easily**
- **Different user accounts may have different preferences**
- **Firmware online upgradeable 24/7**
- **Custom certificate upload**
- **Flexible access sharing modes**
- **VNC screen encryption**
- **Internal firewall**
- **Supports industry-standard networking and management protocols such as TCP/IP and SNMP**
- **Offers secure management options including SSL encryption, SSH tunneling, and RADIUS authentication**
- **Platform independent: can be managed using any Java-enabled Web browser**
- **One remote management point for multiple computers**

B. Package Contents

Your package should contain the following:

- 1 x **Digital KVM via IP** unit
- 1 x Power Adapter
- 1 x AC Cord for Power Adapter
- 1 x User's Manual
- 1 x Rack Mount kit of Standard 19" 1U (for 8/16 ports only)
- 1 x Screw Package (for 8/16 ports only)
- One Set of Foot Pad (for **MNIP/UNIP** series only)
- 1 x **DB9 RS-232 null modem serial cable**

C. Optional

- There are many different lengths for PS/2 or USB cables available:
  1.8, 3.0, 6.0, 10.0, 15.0 m
  The **Serial Supervisor** -- Compatible with **ALL models except MNIP01 / MNIP04**

Serial Supervisor

■ Chapter 2 Your First Time on Digital KVM via IP

A. Quick Start Guide

For this Quick Start Guide, we offer two different easy step-by-step ways, letting you setup this unit very quickly.

Before doing the initial setting:

I. Please make sure the latest Java software downloaded at http://www.java.com on the client computer.

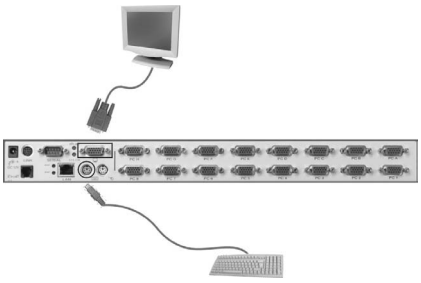
II. Please disable the mouse acceleration on the host computer(s) AND client computer, referring more detailed information on Chapter 2, section B Disabling the Mouse Acceleration on the Host Computer(s) and Client Computer.

The First Way : Using the IP-OSD step-by-step menu (Recommended)

Hardware Necessary for this way

I. A Digital KVM via IP unit with a power adapter
II. A keyboard and monitor
III. A CAT-5 cable with RJ-45 connector

Step 1. Connect a PS/2 keyboard and monitor to the local port of **Digital KVM via IP**.



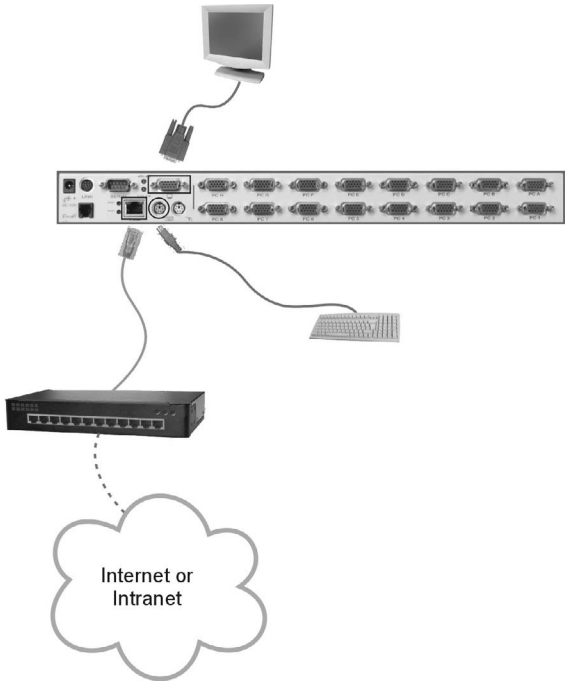
For Stand Alone Unit

or

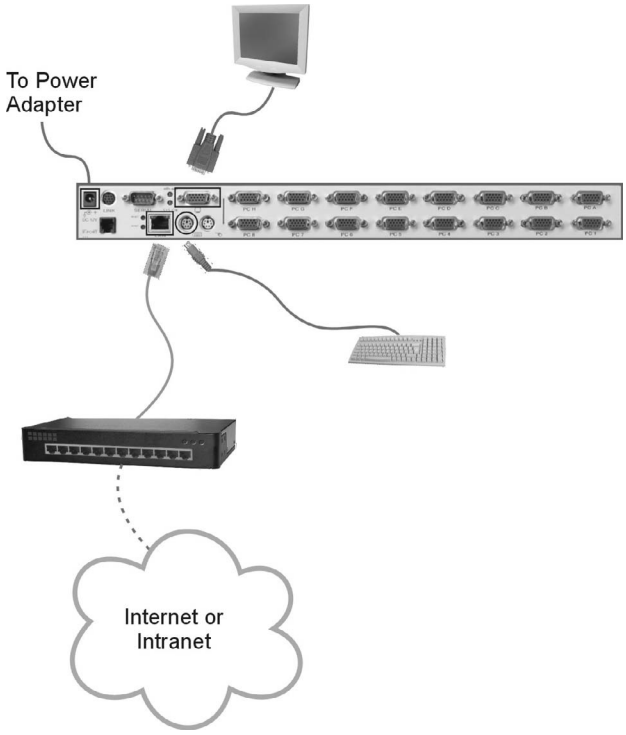
For Module Unit

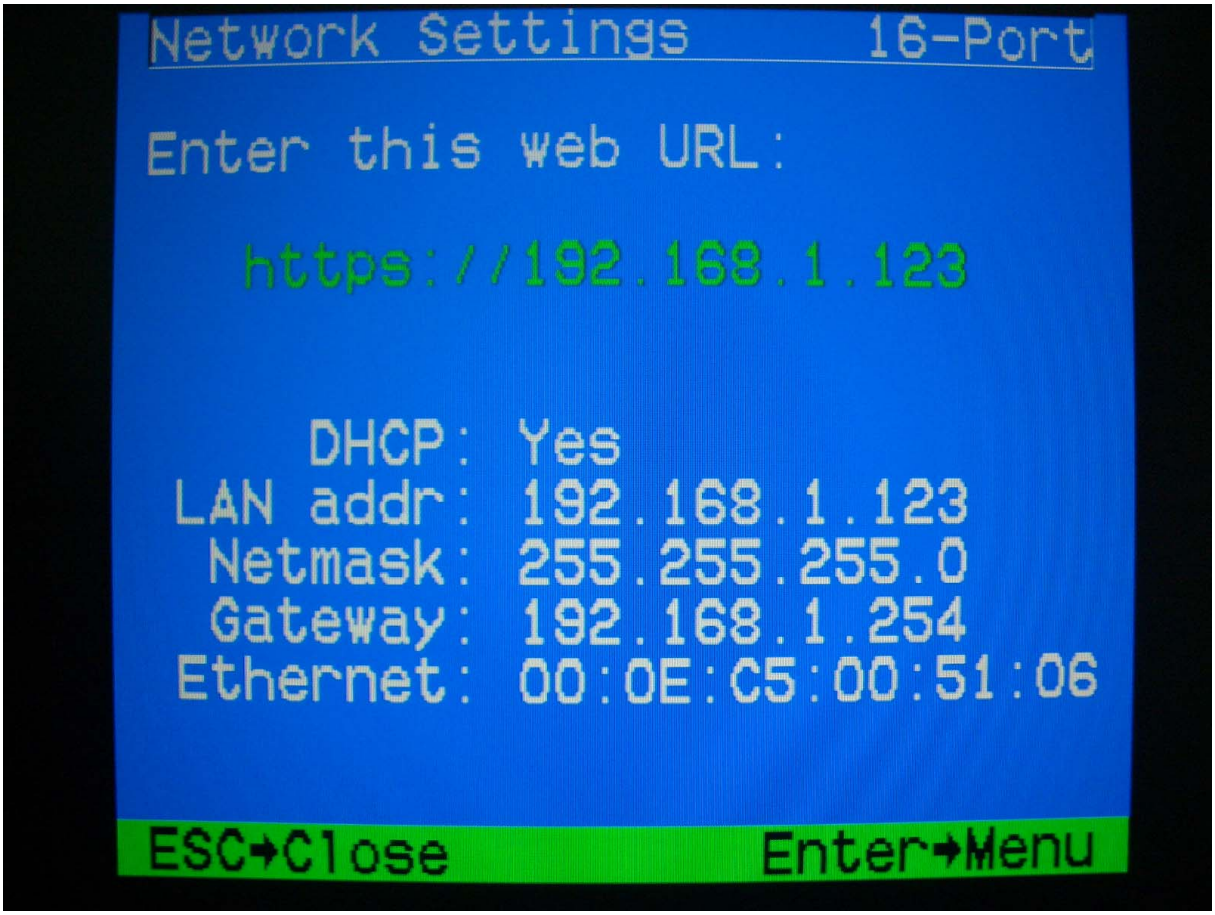
NOTE: for the module unit, please connect it with the LCD console drawer, no need to connect an external keyboard and monitor. The IP-OSD menu comes up automatically on the front console drawer after power up.

Step 2. Connect a CAT-5 cable to the LAN port of **Digital KVM via IP**, making it online.



Step 3. Power up the monitor and **Digital KVM via IP**, the IP-OSD menu comes up automatically; simply follow the step-by-step instructions to finish the initial setup. **<u>If you would like to bring up the menu, please simply use your paperclip or pen to press the "IP SETUP" button.</u>**



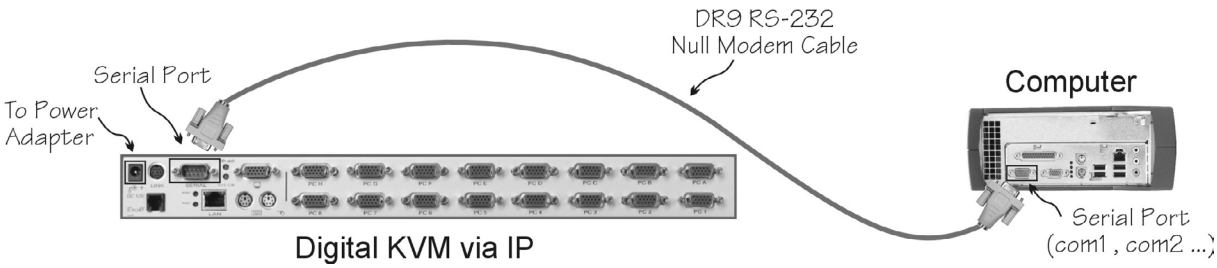


The Second Way: Using the HyperTerminal via Serial Port

Hardware Necessary for this way

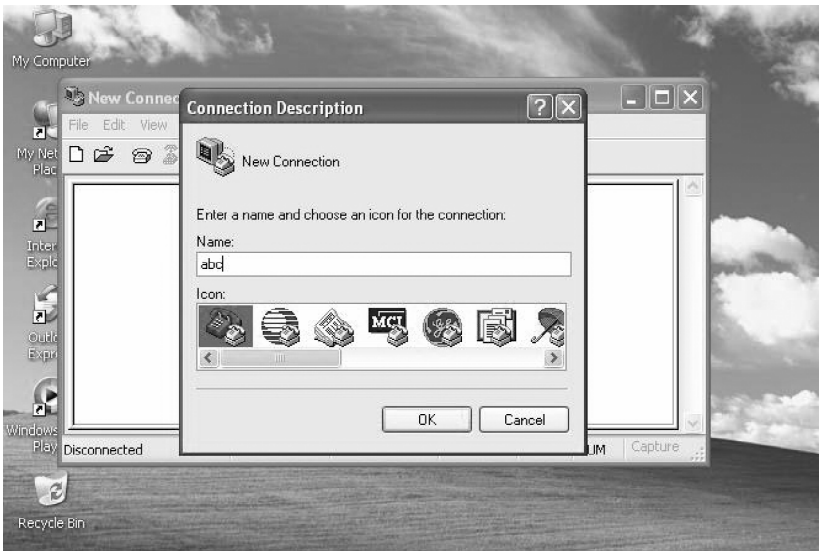
I. A Digital KVM via IP unit with a power adapter
II. A computer with a keyboard, mouse and monitor
III. A CAT-5 cable with RJ-45 connector
IV. A DB9 RS-232 null modem cable

Step 1. Connect the **DB9 RS-232 null modem serial cable** to the **serial port** of **Digital KVM via IP**. And, connect the other end to the serial port (**COM1, COM2…**) of your computer.

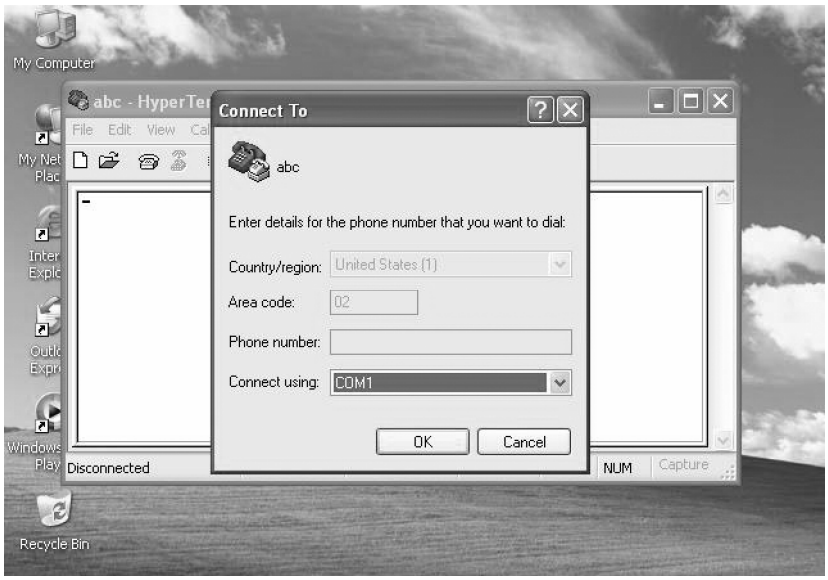


Step 2. From your computer, select "**HyperTerminal**" as following.

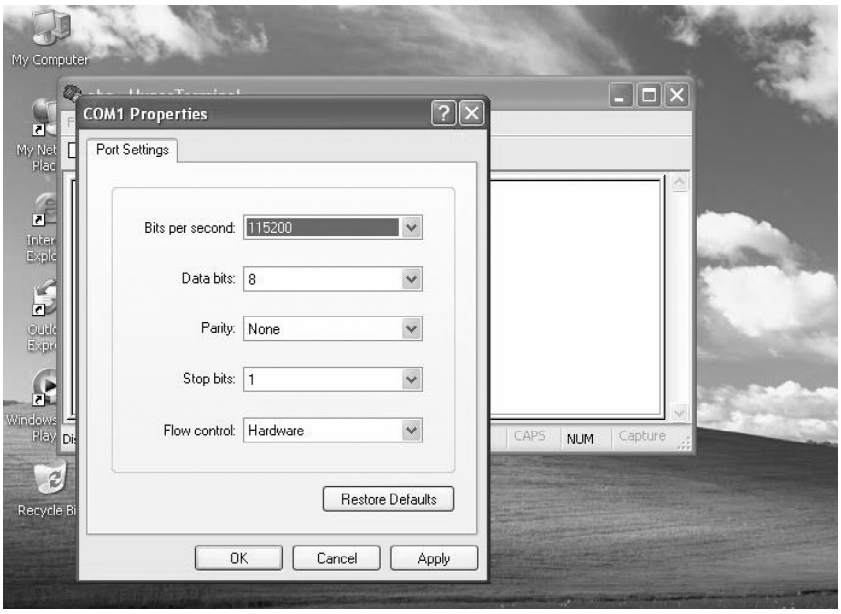
Step 3. If you never setup your **HyperTerminal** before, it will ask you to input your phone area code, please feel free to do so, and then click "**OK**", you will get the following screen. Please type any name you prefer, for example, "**abc**".



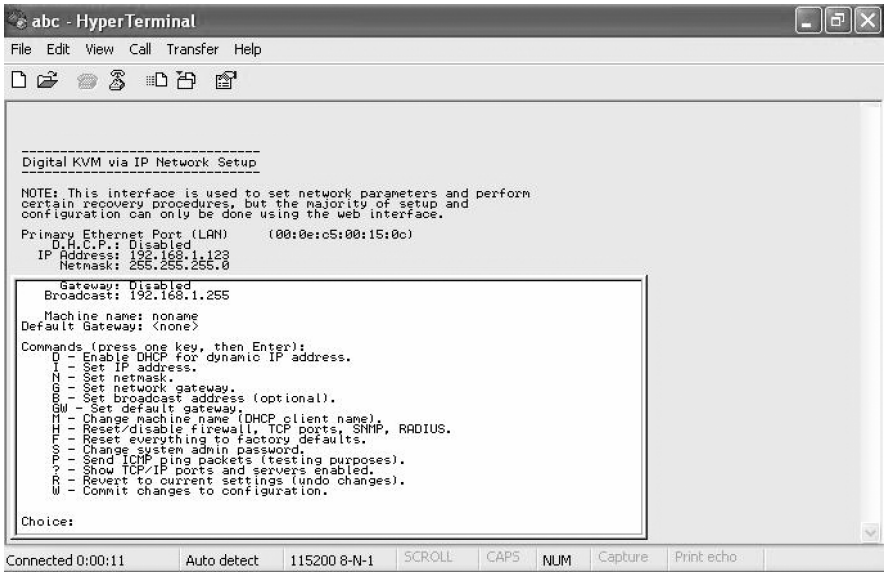
Step 4. Choose the proper serial port you connect, for example, “**COM1**”.



Step 5. Change “**Bits per second**” to **115200**.



Step 6. Press “**Enter**”, you will get the following screen.


abc - HyperTerminal
File Edit View Call Transfer Help
Digital KVM via IP Network Setup
NOTE: This interface is used to set network parameters and perform certain recovery procedures, but the majority of setup and configuration can only be done using the web interface.
Primary Ethernet Port (LAN) (00:0e:c5:00:15:0c)
D.H.C.P.: Disabled
IP Address: 192.168.1.123
Netmask: 255.255.255.0
Gateway: Disabled
Broadcast: 192.168.1.255
Machine name: noname
Default Gateway: <none>
Commands (press one key, then Enter):
D - Enable DHCP for dynamic IP address.
I - Set IP address.
N - Set netmask.
G - Set network gateway.
B - Set broadcast address (optional).
GW - Set default gateway.
M - Change machine name (DHCP client name).
H - Reset/disable firewall, TCP ports, SNMP, RADIUS.
F - Reset everything to factory defaults.
S - Change system admin password.
P - Send ICMP ping packets (testing purposes).
? - Show TCP/IP ports and servers enabled.
R - Revert to current settings (undo changes).
W - Commit changes to configuration.
Choice:
Connected 0:00:11
Auto detect
115200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

Step 7. Follow the instruction on the screen. For example, simply type “I” for setting your IP, type “F” for resetting everything back to factory defaults, and so on. Here is a reminder for you, please type “W” after you made any change.

B. Disabling the Mouse Acceleration on the Host computer(s) and Client Computer

Many operating systems offer a feature called **mouse acceleration** that allows the user to adjust the responsiveness of the cursor on the screen to physical movements of the mouse. While this is usually a beneficial interface enhancement, it can interfere with the operation of the unit and should be disabled on the managed computers before a remote session is attempted. Follow the instructions below to disable mouse acceleration for the operating system installed on each managed computer.

Windows 98 and Windows 2000

1. From the **Control Panel**, click on **Mouse**.
2. From **Mouse Properties**, click on **Motion** tab.
3. Make sure the **Pointer speed bar** is centered and **Acceleration** is set to **None**.

Windows XP and Windows Server 2003

1. From the **Control Panel**, click on **Mouse**.
2. Go to "**Pointer Options** " and turn off "**Enhance Pointer Precision**."
3. Make sure that the **Pointer speed bar** is centered.

Linux, Unix and X-Windows

1. Add this command to your xinitrc, xsession or other startup script:

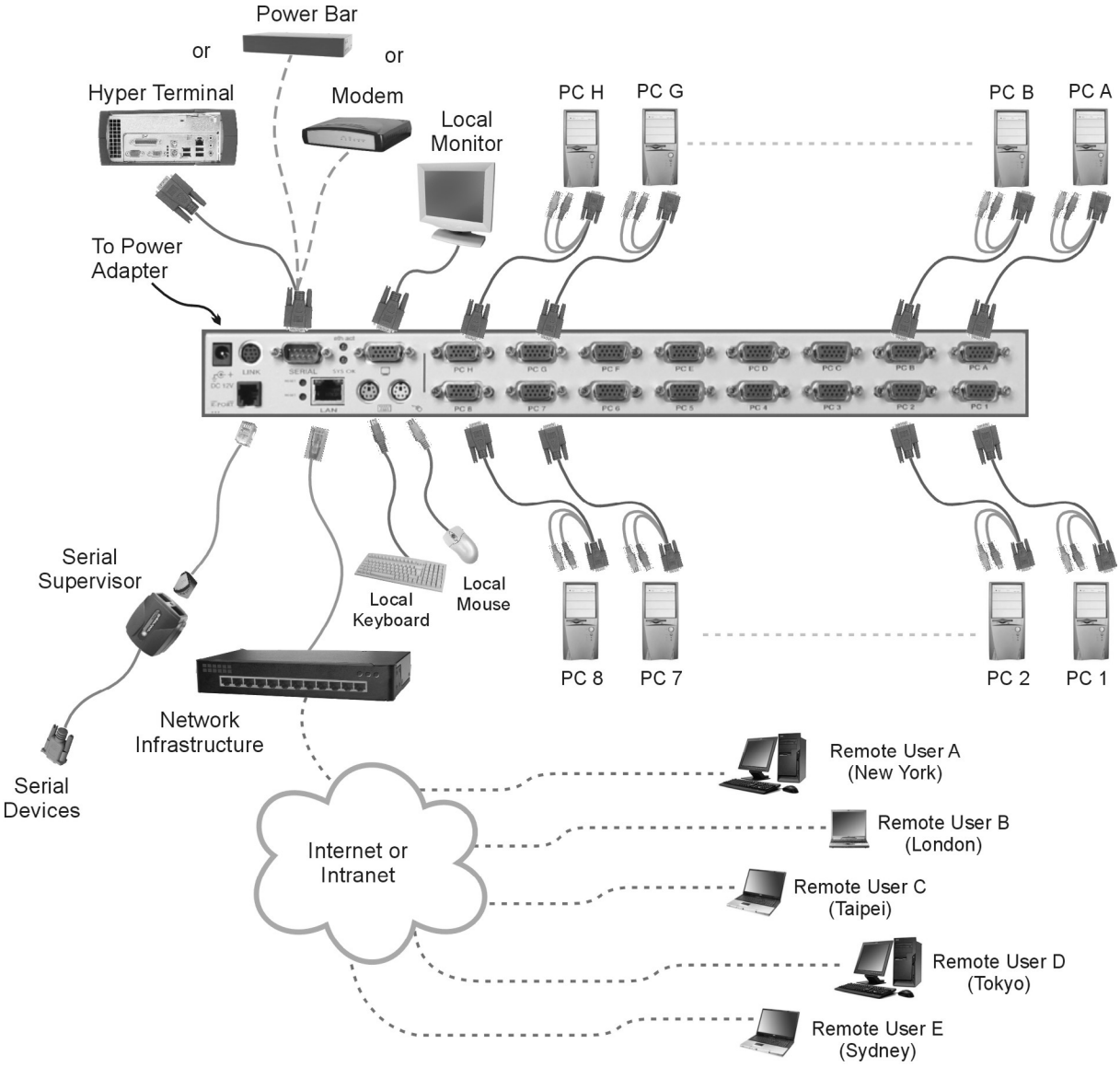
xset m 0/0 0

Sun Solaris

1. Add this command to your xinitrc, xession or other startup script:

xset m 1/1 0

C. How to Connect your Digital KVM via IP



Example of 16-port **Digital KVM via IP** Connection

UNIP/MNIP16 and WMM/WUM116D: Ports **PC 1~8/A~H**
UNIP/MNIP08 and WMM/WUM108D: Ports **PC 1~8 only**
UNIP/MNIP04: Ports **PC 1~4 only**
MNIP01and WMM/WUM 001: 1 Port

The restrictions on functions such as cascading and the assignment of master and slave units also apply to all versions of the product.

1. Ensure that the **Digital KVM via IP** unit and the computers to be managed are powered off.
2. If desired, mount the unit in a standardized rack or cabinet.
3. Connect a standard straight-through Ethernet patch cable to the **LAN** port on the rear panel of the unit.
4. Connect the opposite end to your **network hub**, **switch**, or **terminated wall outlet**.

5. If you wish to use the product as a local console, connect a standard keyboard (purple connector) and mouse (green connector) to the PS/2 ports, as marked on the rear panel.
6. Connect a VGA monitor to the video-out port on the rear panel of the unit.
7. (a) **If you are using PS/2 connections to your managed computers**, connect the end of the **CBM180H** cable that has three connectors (keyboard, video, mouse) to the keyboard, mouse, and VGA Out ports on a computer (often a server or other critical system). Connect the opposite end (with a single VGA-style connector) to one of the **PC 1~8**/**A~H** ports on the rear panel of the **Digital KVM via IP**. Repeat this procedure for each PS/2-enabled managed computer. You will be able to add additional managed computers later with the **Digital KVM via IP** powered on.

   (b) **If you are using USB connections to your managed computers**, connect the end of the **CBM180UH** cable that has two connectors (USB, video) to an available USB port and VGA Out port on the computer (often a server or other critical system). Connect the opposite end (with a single VGA-style connector) to one of the **PC 1~8**/**A~H** ports on the rear panel of the **Digital KVM via IP**. Repeat this procedure for each USB-enabled managed computer. You will be able to add additional managed computers later with the KVM powered on.
8. (For 8/16 ports only) please mount the brackets with the unit as following figure.

9. Power on the **Digital KVM via IP** by connecting the AC adapter to a suitable power source and connecting the opposite end to the **DC 12V** port on the rear panel of the unit.
10. Power on each of the managed computers, observing normal startup procedures.

NOTE: You can choose to mix managed computers connected via PS/2 and USB connections as necessary with no impact on features or functionality.

NOTE: Steps 5 and 6 are necessary only if you wish to have the ability to manage the KVM and its computers locally (i.e. not over the Internet or LAN). While not required, adding these devices is highly recommended for ease of administration.

NOTE: The KVM also has the ability to “cascade” multiple KVMs to increase the total number of possible managed computers. If you wish to take advantage of this feature, refer to the section “Cascade Configuration” in this manual.

D. Access your Digital KVM via IP and Remote Control the Host computer(s)

As soon as you finish the above initial settings and connections, congratulations! You are ready to enjoy remote control the host computer(s) from any corner around the whole world! Simply open up the web browser and type the IP you already setup in the Quick Start Guide and then type the right username and password. That it! You're successful to access your **Digital KVM via IP**! As you login the **Digital KVM via IP** with the right username and password, you will get the following screen:

Please simply double click on the small square window in the middle of the screen. You'll get the VNC screen.(**You may need to upgrade or download your Java support in your browser before using the VNC screen to remote control the host computer(s)**; however, most modern browsers come with a version of Java that is compatible with this application.) That is, you will see the screen of the host computer(s). Now, you can fully control the host computer(s) *remotely* like you present at the host computer(s) location physically, sitting in front of the host computer(s)! Certainly, if you would like to log out your **Digital KVM via IP**, please simply click on the icon of "**Logout**" on the top of screen!

■ Chapter 3 Advanced Operations

The Web interface is the most intuitive way to configure the **Digital KVM via IP**. It also offers a Java-based VNC client that you can use to control the managed computers from a remote location. The **Digital KVM via IP** supports any industry-standard **HTML** Web browser. You can access the Web interface by opening your Web browser and entering the IP address of the unit you wish to access/configure. The IP address will be either

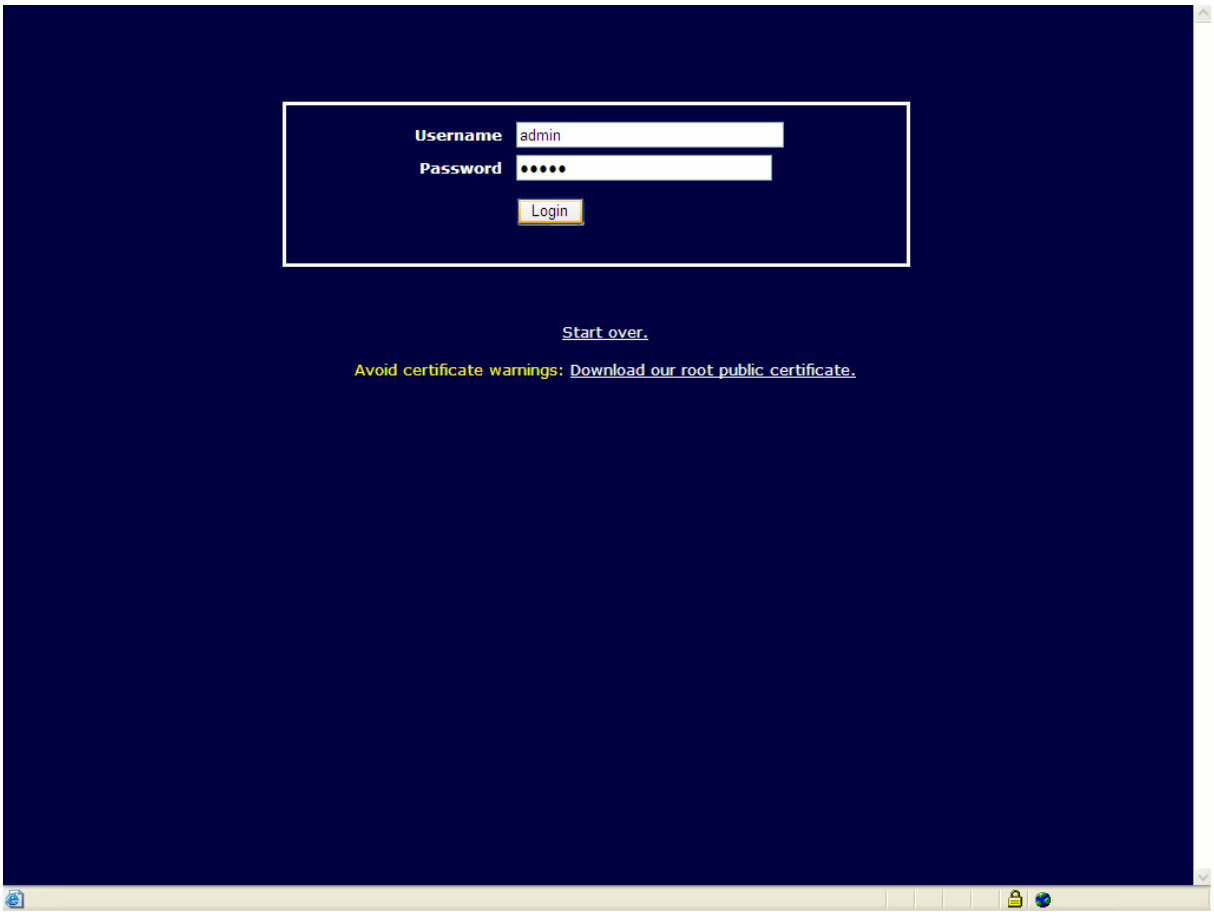
a) the address assigned for the **LAN** port by your **DHCP server** as identified in the previous section,
or
b) the fixed IP address you setup, see Quick Start Guide for more information. Again, the default IP address of the LAN port of **Digital KVM via IP** is **https://192.168.1.123**. **Please remember to add "s" after "http" which means this web page is under SSL 128 bits encryption protection.**

NOTE: Only the "admin" account have rights to change all of the following settings.

A. How to login the Digital KVM via IP

Step 1: The Login Screen

Before you can access the Web configuration interface, you must enter a **username** and **password**. The **default** username and password as shipped from the factory is username **admin** with a password of **admin**.



NOTE: Before the login screen appears, your Web browser may display a warning about an invalid security certificate. This does not affect the security of your data in any way. **Whenever you are prompted about a certificate security problem by your browser or the Java VNC client, always choose the option to continue.** .

Step 2: The Home Screen

The Home screen serves two functions. First, it is a place to check the status of the unit, view essential system information, and capture screen shots from the managed computers. Second, it is where you can start the integrated Java VNC client to interact with the managed computers by clicking on the large screen shot or choosing one of the VNC client links.

B. Configure your Digital KVM via IP

The Home Screen

The menu list on the left hand side allows you to access all of the features to perform the configuration of the **Digital KVM via IP**.

Each item is described in details as following:

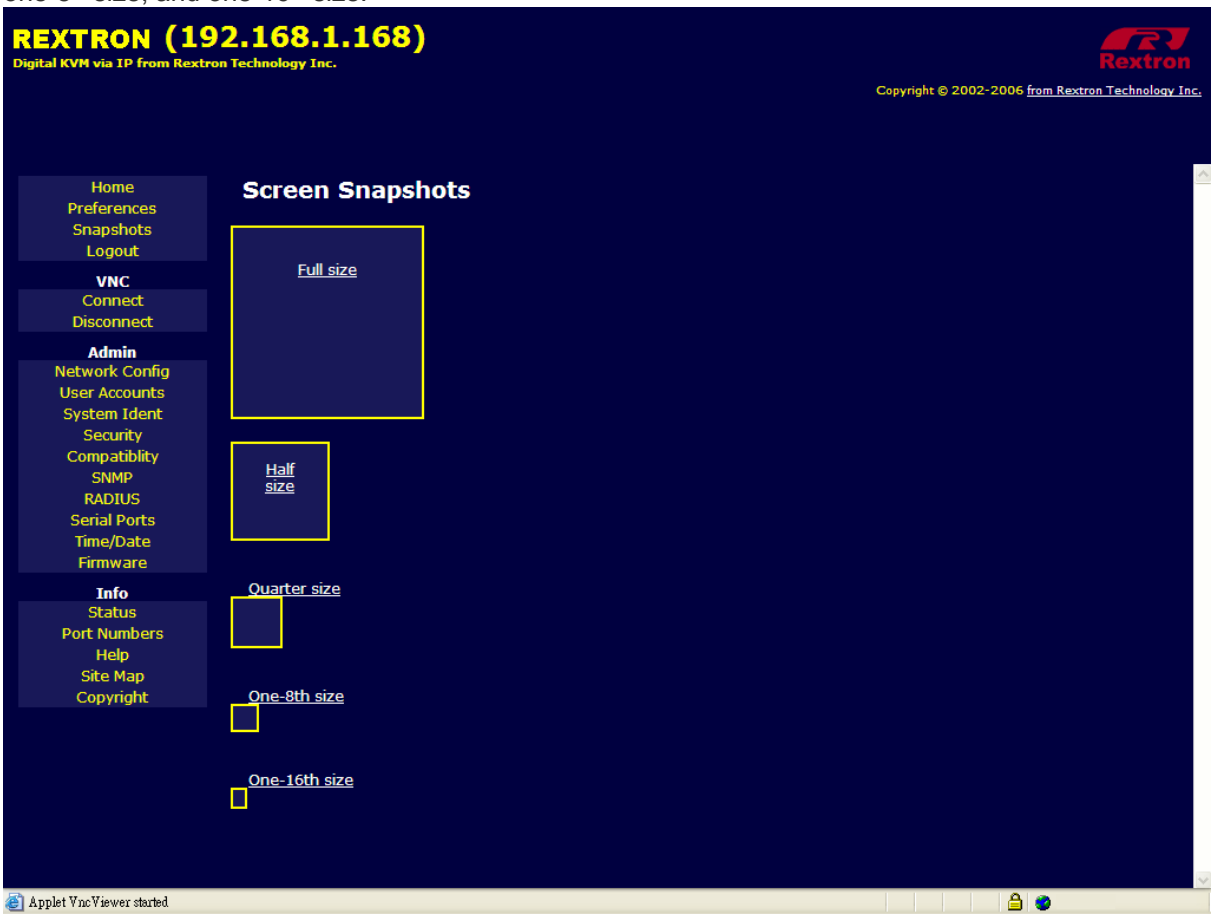
I. How to Setup Personal Preferences

Different user accounts may have different personal preferences. It might be a good idea to have a login account for “local” access and a different one for “remote” access. The “local” account would select 16-bit color, max bandwidth, and so on. And, the “remote” account would select 8-bit color, low bandwidth, no splash screen and require encryption. By selecting the correct login depends on the application (i.e. login from home over WAN versus LAN login). As the following image shown, the current user preferences are listed here as follows. You may change any of them and save with the button below. Most of these preferences affect how the VNC client and server interact.

REXTRON (192.168.1.168)
Digital KVM via IP from Rextron Technology Inc.
Rextron
Copyright © 2002-2006 from Rextron Technology Inc.
Home
Preferences
Snapshots
Logout
VNC
Connect
Disconnect
Admin
Network Config
User Accounts
System Ident
Security
Compatiblity
SNMP
RADIUS
Serial Ports
Time/Date
Firmware
Info
Status
Port Numbers
Help
Site Map
Copyright
User preferences
Open VNC connection immediately on web login
No (use buttons to start VNC)
Yes (VNC started on login)
Force bandwidth mode
Auto (not forced)
Min (slowest/least traffic)
Average
Max (fastest/most traffic)
Reduce network traffic by limiting colors
8-bit (256 colors)
12-bit (4096 colors)
16-bit (default: 65536 colors)
VNC Callback instead of Java VNC
No (use Java client)
Yes (use VNC callback to native client)
Encrypt VNC connection
Encrypt over Internet only
Always Encrypt
Never Encrypt
Optimize for full-screen VNC
No (normal)
Yes (don't show Bribar)
Skip welcome window on VNC connection
No (normal)
Yes (skip welcome window)
Save Changes
Default Values
Reset all
User preferences
Your current user preferences are listed here. You may change any of them and save with the button below.
Most of these preferences affect how the VNC client and server interact.
Open VNC connection immediately on web login
Start a VNC connection immediately after login to the web server. The connect button does not need to be used.
Force bandwidth mode
By default, the initial connection performance (RTT) is measured and used to select whether to optimize a high bandwidth connection or low. If the connection improves, the bandwidth used will be adjusted. You can override this while the connection is operating. Use this preference to override auto mode and force the B/W mode.
Reduce network traffic by limiting colors
Network traffic (bandwidth) may be reduced by reducing the image quality. We do not recommend 12-bit mode but provide it here as a middle ground.
VNC Callback instead of Java VNC
If you have a VNC client 'listening' on your work station and would prefer to use that instead of Java client, enable this option.
Encrypt VNC connection
By default we will use the cleartext (not encrypted) connection when the network connection looks like a 'local link' (ie. same IP subnet). Encrypted mode is the default on Internet connections. Use this control to force the use of the encrypted VNC connection or no encryption. Only affects Java VNC client.
Optimize for full-screen VNC
This control hides the Bribar
java.lang.NullPointerException

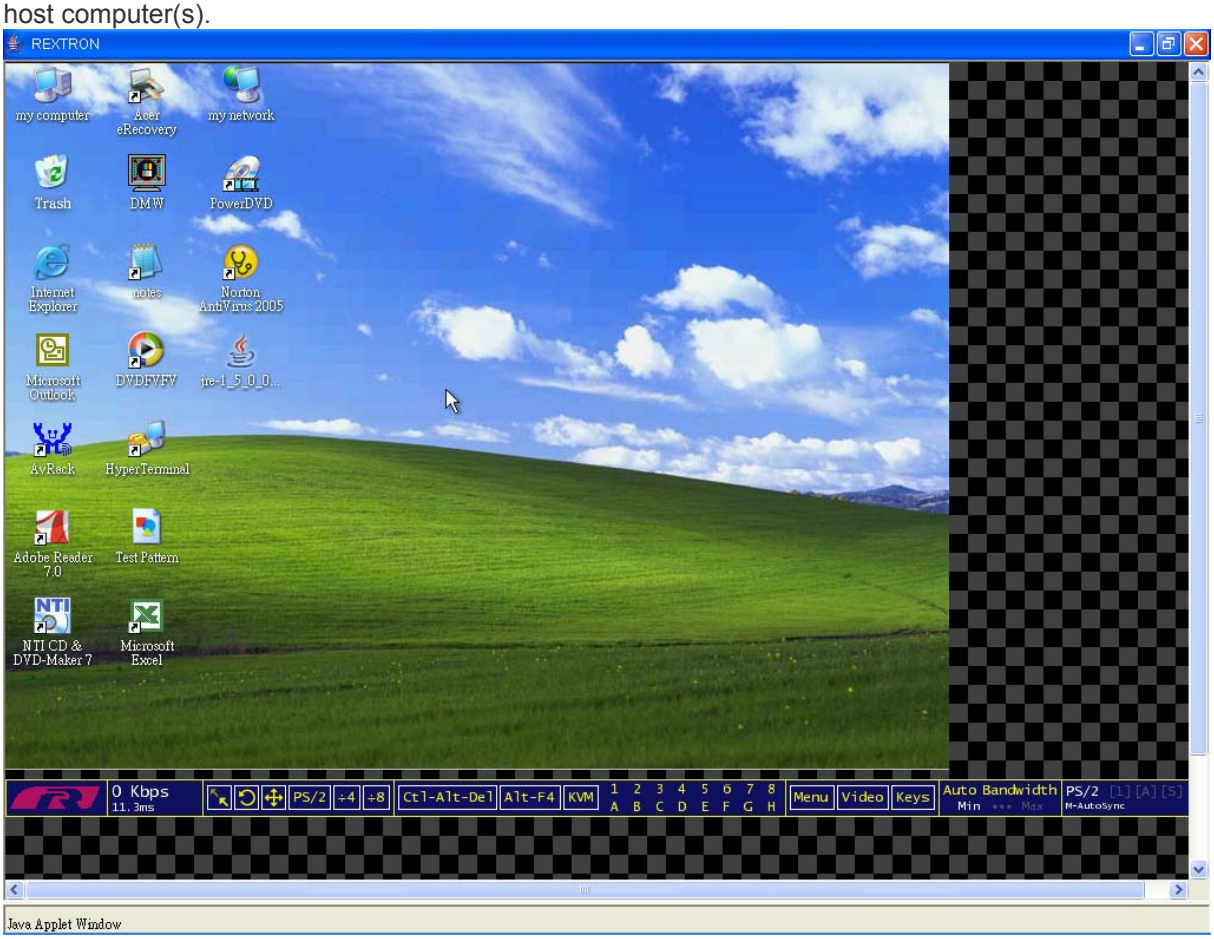
II. How to Get the Snapshots

As the following image shown, the user can get the screen snapshot of full size, half size, quarter size, one-8th size, and one-16th size.



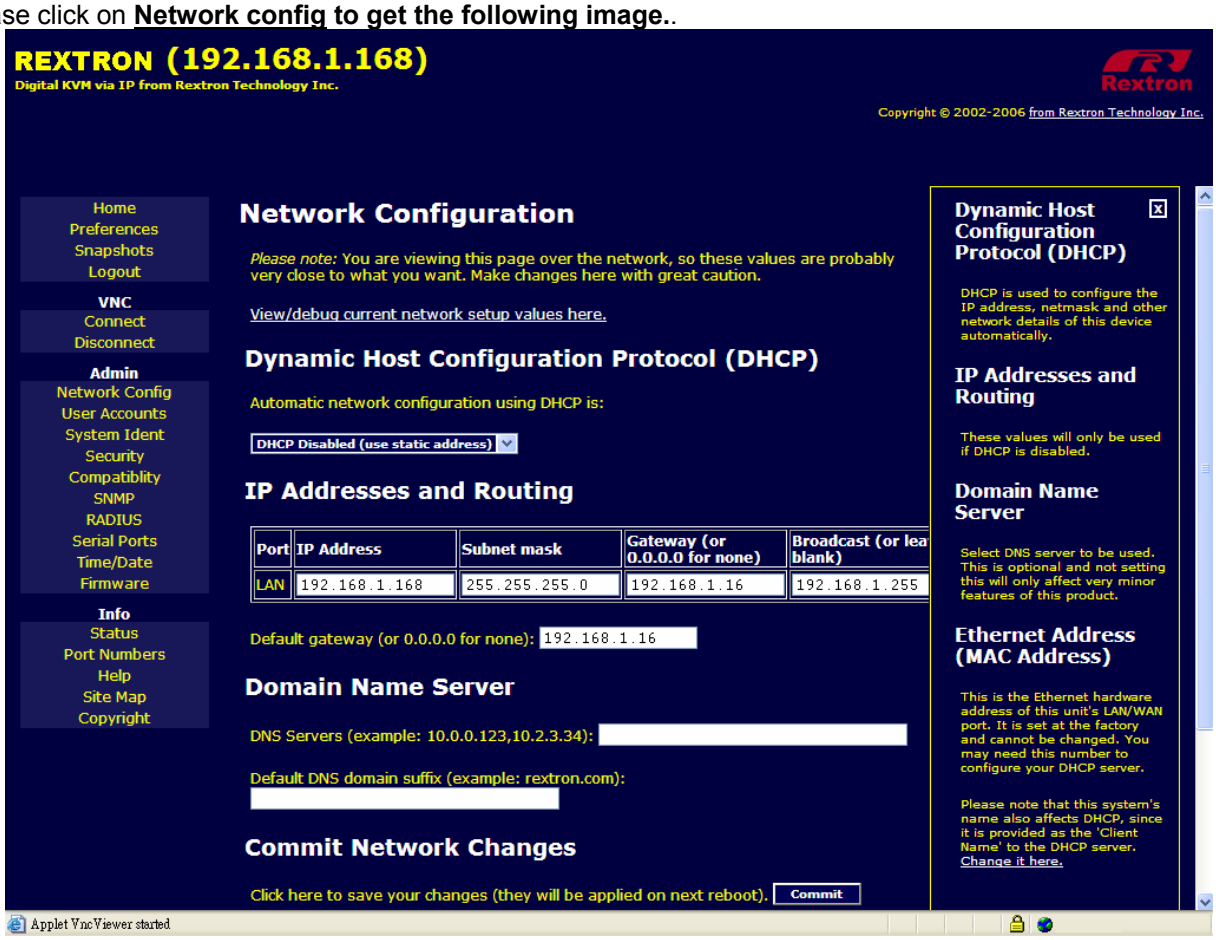
III. How to Remote Control the Host Computer(s)

Please simply click the “VNC Connect” to get the screen of host computer as the following image shown. From here, you get the fully control on the host computer like you physically sit in front of the host computer(s).

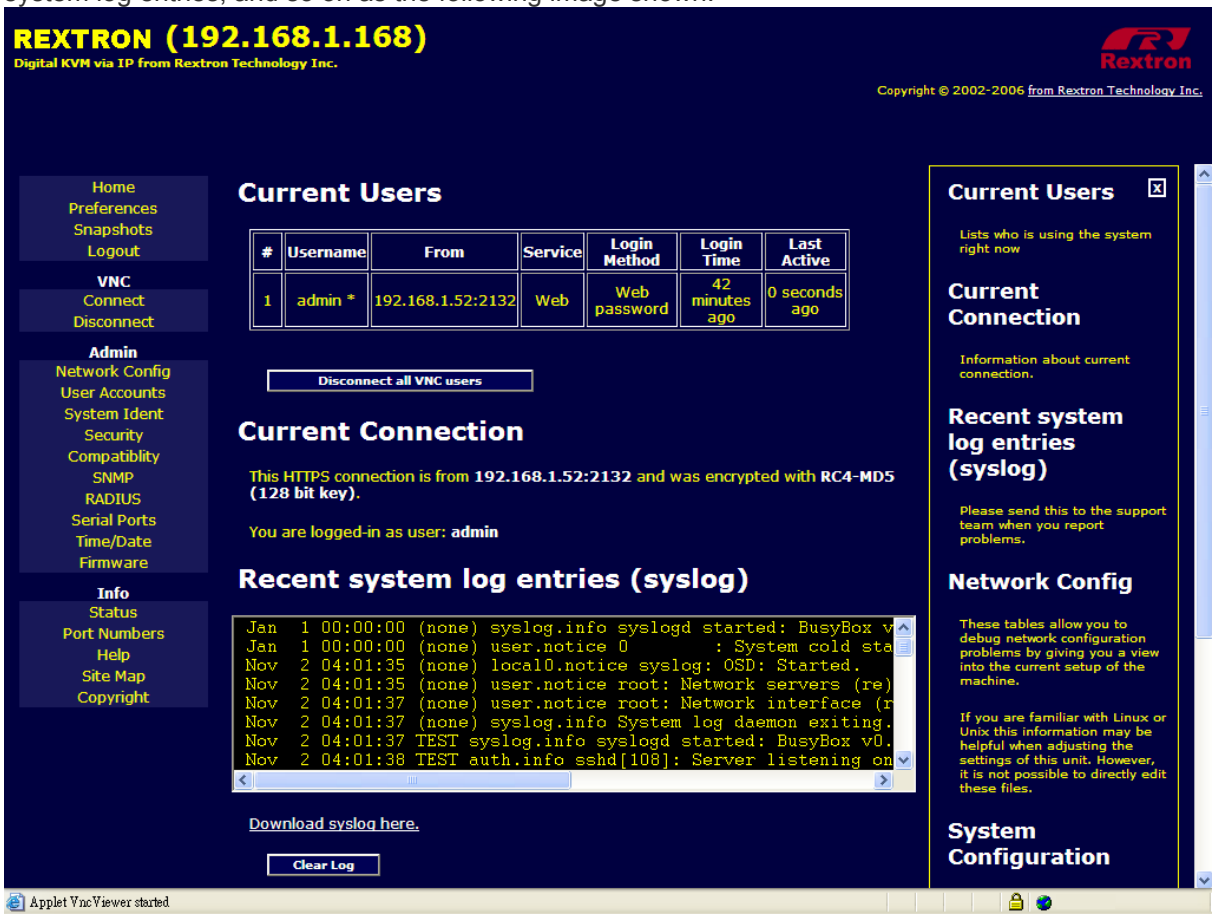


IV. How to Setup the IP Address for your Digital KVM via IP

Please click on **Network config to get the following image.**.


REXTRON (192.168.1.168)
Digital KVM via IP from Rextron Technology Inc.
Rextron
Copyright © 2002-2006 from Rextron Technology Inc.
Home
Preferences
Snapshots
Logout
VNC
Connect
Disconnect
Admin
Network Config
User Accounts
System Ident
Security
Compatiblity
SNMP
RADIUS
Serial Ports
Time/Date
Firmware
Info
Status
Port Numbers
Help
Site Map
Copyright
Network Configuration
Please note: You are viewing this page over the network, so these values are probably very close to what you want. Make changes here with great caution.
View/debug current network setup values here.
Dynamic Host Configuration Protocol (DHCP)
Automatic network configuration using DHCP is:
DHCP Disabled (use static address)
IP Addresses and Routing
Port
IP Address
Subnet mask
Gateway (or 0.0.0.0 for none)
Broadcast (or lea blank)
LAN
192.168.1.168
255.255.255.0
192.168.1.16
192.168.1.255
Default gateway (or 0.0.0.0 for none): 192.168.1.16
Domain Name Server
DNS Servers (example: 10.0.0.123,10.2.3.34):
Default DNS domain suffix (example: rextron.com):
Commit Network Changes
Click here to save your changes (they will be applied on next reboot).
Commit
Dynamic Host Configuration Protocol (DHCP)
DHCP is used to configure the IP address, netmask and other network details of this device automatically.
IP Addresses and Routing
These values will only be used if DHCP is disabled.
Domain Name Server
Select DNS server to be used. This is optional and not setting this will only affect very minor features of this product.
Ethernet Address (MAC Address)
This is the Ethernet hardware address of this unit's LAN/WAN port. It is set at the factory and cannot be changed. You may need this number to configure your DHCP server.
Please note that this system's name also affects DHCP, since it is provided as the 'Client Name' to the DHCP server. Change it here.
Applet VncViewer started

View / debug current network setup values here
This link allows you to monitor the records about current login users, current connection, recent system log entries, and so on as the following image shown.


REXTRON (192.168.1.168)
Digital KVM via IP from Rextron Technology Inc.
Rextron
Copyright © 2002-2006 from Rextron Technology Inc.
Home
Preferences
Snapshots
Logout
VNC
Connect
Disconnect
Admin
Network Config
User Accounts
System Ident
Security
Compatiblity
SNMP
RADIUS
Serial Ports
Time/Date
Firmware
Info
Status
Port Numbers
Help
Site Map
Copyright
Current Users
Username From Service Login Method Login Time Last Active
1 admin * 192.168.1.52:2132 Web Web password 42 minutes ago 0 seconds ago
Disconnect all VNC users
Current Connection
This HTTPS connection is from 192.168.1.52:2132 and was encrypted with RC4-MD5 (128 bit key).
You are logged-in as user: admin
Recent system log entries (syslog)
Jan 1 00:00:00 (none) syslog.info syslogd started: BusyBox v
Jan 1 00:00:00 (none) user.notice 0 : System cold sta
Nov 2 04:01:35 (none) local0.notice syslog: OSD: Started.
Nov 2 04:01:35 (none) user.notice root: Network servers (re)
Nov 2 04:01:37 (none) user.notice root: Network interface (r
Nov 2 04:01:37 (none) syslog.info System log daemon exiting.
Nov 2 04:01:37 TEST syslog.info syslogd started: BusyBox v0.
Nov 2 04:01:38 TEST auth.info sshd[108]: Server listening on
Download syslog here.
Clear Log
Current Users
Lists who is using the system right now
Current Connection
Information about current connection.
Recent system log entries (syslog)
Please send this to the support team when you report problems.
Network Config
These tables allow you to debug network configuration problems by giving you a view into the current setup of the machine.
If you are familiar with Linux or Unix this information may be helpful when adjusting the settings of this unit. However, it is not possible to directly edit these files.
System Configuration
Applet VncViewer started

Dynamic Host Configuration Protocol (DHCP)

Automatic network configuration using **DHCP** is: **Enabled/Disabled.**
This feature applies to the **LAN** port on the rear panel, and is enabled by default. When enabled, the unit will automatically configure itself with an IP address when a **DHCP** server is present. When disabled, the **LAN** port will use the values assigned to it on the **IP Addresses and Routing** table below.

IP Addresses and Routing
This table allows you to assign IP information for the **LAN** port. If you are using **DHCP**, the values for the **LAN** port will be filled in automatically and any changes made will not affect the setup.

Domain Name Server (optional)
This section allows you to specify DNS servers and the default DNS domain suffix in use on the network. If **DHCP** is enabled, some of these values may be supplied automatically.

Commit Network Changes
Clicking the **Commit** button applies any changes made on the page to the configuration, but leaves the old settings active until the next time the unit restarts. Clicking **Make changes effective now** applies the changes and restarts the unit so the new settings take effect immediately.

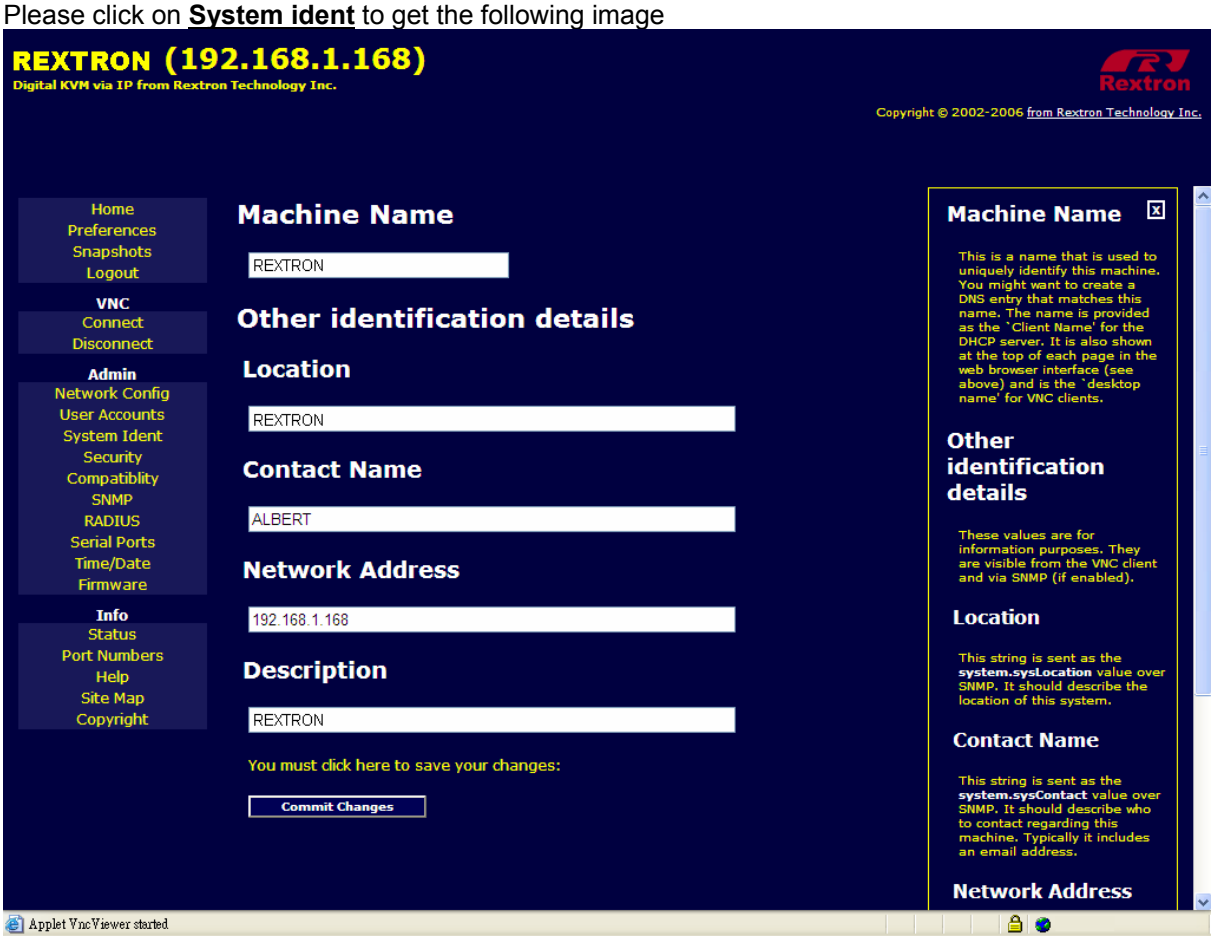
V. How to Edit the User Accounts

Please click on **User Accounts** to get the following image.

This menu will allow you to add accounts other than **admin** to the system. These accounts will not have the authority to change settings, but can access the Web interface and log in the VNC console. Selecting **Delete** permanently removes the user from the system. If you enter values for a user that does not already exist under **Edit User Details**, the system will create that user for you when you click **Record changes**. If the user already exists, you will change the password for that user.

VI. How to Setup your Digital KVM via IP System Identification

Please click on **System ident** to get the following image


REXTRON (192.168.1.168)
Digital KVM via IP from Rextron Technology Inc.
Rextron
Copyright © 2002-2006 from Rextron Technology Inc.
Home
Preferences
Snapshots
Logout
VNC
Connect
Disconnect
Admin
Network Config
User Accounts
System Ident
Security
Compatiblity
SNMP
RADIUS
Serial Ports
Time/Date
Firmware
Info
Status
Port Numbers
Help
Site Map
Copyright
Machine Name
REXTRON
Other identification details
Location
REXTRON
Contact Name
ALBERT
Network Address
192.168.1.168
Description
REXTRON
You must click here to save your changes:
Commit Changes
Machine Name
This is a name that is used to uniquely identify this machine. You might want to create a DNS entry that matches this name. The name is provided as the `Client Name' for the DHCP server. It is also shown at the top of each page in the web browser interface (see above) and is the `desktop name' for VNC clients.
Other identification details
These values are for information purposes. They are visible from the VNC client and via SNMP (if enabled).
Location
This string is sent as the system.sysLocation value over SNMP. It should describe the location of this system.
Contact Name
This string is sent as the system.sysContact value over SNMP. It should describe who to contact regarding this machine. Typically it includes an email address.
Network Address
Applet VncViewer started

Right here, you can define the following details:

- machine name
- location
- contact name
- network address
- description

These details are useful for the DHCP servers, SNMP agents, and VNC clients. While these values do not affect the operation of the unit, they make it easier to manage on the network.

VII. How to Strengthen your Digital KVM via IP System Security

Please click on **Security** to get the following image.

REXTRON (192.168.1.168)
Digital KVM via IP from Rextron Technology Inc.
Rextron
Copyright © 2002-2006 from Rextron Technology Inc.
Home
Preferences
Snapshots
Logout
VNC
Connect
Disconnect
Admin
Network Config
User Accounts
System Ident
Security
Compatiblity
SNMP
RADIUS
Serial Ports
Time/Date
Firmware
Info
Status
Port Numbers
Help
Site Map
Copyright
Security Profile
Administrator Password
Set admin password
Idle Session Timeout
15
minutes
Commit Change
Internal Firewall Setup
Disabled - Ignore source IP address (default)
Accept:
Reject:
WARNING: Be careful not to lock yourself out! Be certain that 192.168.1.52 will be accepted by your filter!
Commit Changes
VNC Password Policy
Disabled - Use regular VNC passwords (default)
Trust SSH Tunnels
Trust SSH Tunnels (default)
Access Sharing Policy
Enforce single-user access policy (visible screen)
Local User Lockout
Disabled - Local user always has access (default)
Security Profile
Administrator Password
This is the administrator password (AKA root, superuser). You must have used it to get here.
The administrator's password can be changed here. However, the user name for this account cannot be changed: The system will accept either `root', `admin', or `administrator' as the name of this account.
Add or change other user accounts here.
Idle Session Timeout
When a login session is left unused for some time, it is prudent to disconnect the user. This applies to web login sessions (via cookies) and SSH logins.
This feature may be disabled by setting the value to zero.
Internal Firewall Setup
As an additional layer of protection, we offer an internal firewall. When this feature is enabled, connections will only be accepted from listed hosts. All packets other than those from the hosts you list will be ignored (dropped). This makes the system invisible to them.
You may either list addresses to accept, or list those that you wish to reject. (It doesn't make sense to do both.) Just list specific IP addresses (ie. 10.0.0.23,10.1.2.3), or net ranges (ie. 192.168.0.0/16), or host names (ie. evil.hacker.com). Separate multiple values with commas.
VNC Password Policy
Applet VncViewer started

This menu allows you to configure a number of settings, including:

Administrator Password

The administrator can change the default password for admin (recommended). Read and consider the comments and instructions on this menu before making any changes, as changing these features could make the unit inaccessible through Web configuration (i.e. due to firewall filtering). **NOTE** that any password changes you make will have to be entered in duplicate to prevent the chance for error.

Idle Session Timeout
When a login session is left unused for some time, it is prudent to disconnect the user. This applies to web login sessions (via cookies) and SSH logins. This feature may be disabled by setting the value to zero.

Internal Firewall Setup
As an additional layer of protection, we offer an internal firewall. When this feature is enabled, connections will only be accepted from listed hosts. For example, the administrator can key in 10.1.0.1/240 in "Accept" filed, that is, the IP of the client's computer between 10.1.0.1 and 10.1.0.240 allows accessing the **Digital KVM via IP** with the right username and password. On the other hand, the user can key in 192.168.1.0/20, for example, in "Reject" field, that is the IP of the client's computer between 192.168.1.0 and 192.168.1.20 will be rejected to access the **Digital KVM via IP**. This makes the **Digital KVM via IP** invisible to them. There are 3 ways to key in the IP addresses:

1. Specific IP addresses: for example, 10.1.0.1, 10.1.0.5,….

2. Net Range: for example, 10.1.0.1/240

3. Host Names: for example, yahoo.com, google.com,…

WARNING: Be careful NOT to lock yourself out! Be certain that your IP will be accepted by your filter.

VNC Password Policy
When a new VNC connection is established, the remote user must be authenticated. Standard VNC protocol does not support "username"; it only supports passwords. As long as all users have unique passwords, we can infer which user is connecting based on the password provided. Alternatively, you may enable a second login screen that will require a valid username and password. This is done after the VNC connection is established using menus and prompts generated by the firmware. We call this second method "fancy login".
If it is enabled, fancy login will be required from Java VNC clients as well, which is unfortunate because the one-time password scheme cannot be used, and Java VNC clients have already logged into the web server securely. Also, VNC normally encrypts passwords and uses a challenge/hashed response system that is more secure than the fancy login method. This isn't a concern if the entire connection is encrypted with SSH or SSL however.

Trust SSH Tunnels
If the incoming VNC connection is coming in over an SSH tunnel, the SSH user / password combination is used and no password is required. Disable this behavior if you suspect that your SSH client machine is not secure and you are concerned that your SSH tunnels may be used by other people.

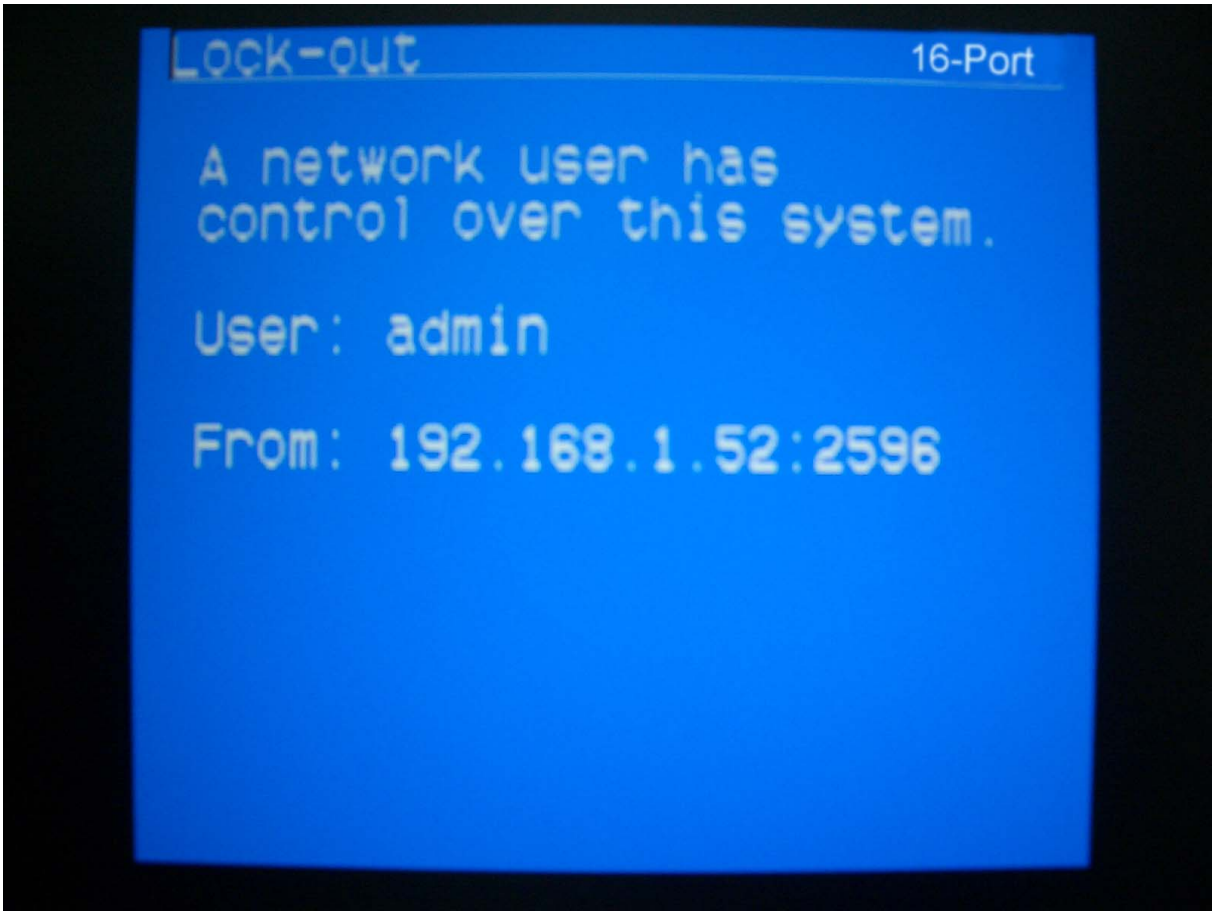
Access Sharing Policy
There are 3 modes available:
1. **Disables – Use regular give/take method (default)**: by default we allow all users to take keyboard and mouse control of the system (after connecting via VNC) using a single mouse click.
2. **Enforce single user access policy (visible screen)**: for some circumstances require more strict control of this capability, the admin user can select this mode for the highest priority access. With a single-user access policy, only one user may control the host computer(s). New connections are permitted, but the admin user. They will be able to view the screen ONLY, but control the host computer(s). Once the first user disconnects (or otherwise gives up control), the second user will be able to access the system immediately.
3. **Enforce single user access policy (blank screen contents)**: for some circumstances require more strict control of this capability, the admin user can select this mode for the highest privacy; no one can see what the admin user is doing from the VNC screen. That is,

the admin user can blank the screen contents when another user is connected but not controlling the keyboard and mouse.
With a single-user access policy, only one user may control the system. New connections are permitted, but the admin user, they will NOT be able to see or even control the host computer(s). Once the first user disconnects (or otherwise gives up control), the second user will be able to access the system immediately.

Local User Lockout
There are 2 modes available:

1. **Disable – Local user always has access (default)**: under this mode, the local user has the access right to control the host computer(s).

2. **Enable – Network user given priority:** under this mode, the local user has NO right to control the host computer(s). And on the screen, there is an IP-OSD menu pops up as the following image shown. The local user can't see and do anything, only this IP-OSD menu shown on the screen. That is, the admin user can select this mode to lock out the local user. Please keep in mind that the local user has no way to take control away from the network user, so an unattended VNC session can cause a problem. Under this situation, if you are locked-out of the system because someone has left a VNC session connected and cannot be reached though other means, the admin user may close all VNC connections. See the Status page to access this feature.



VIII. How to Setup your Digital KVM via IP with the External Power Bar and Keyboard Mapping

Please click on **Compatibility** to get the following image.

REXTRON (192.168.1.168)
Digital KVM via IP from Rextron Technology Inc.
Rextron
Copyright © 2002-2006 from Rextron Technology Inc.
Home
Preferences
Snapshots
Logout
VNC
Connect
Disconnect
Admin
Network Config
User Accounts
System Ident
Security
Compatiblity
SNMP
RADIUS
Serial Ports
Time/Date
Firmware
Info
Status
Port Numbers
Help
Site Map
Copyright
Keyboard Mapping (for localization)
Select keyboard layout: Generic or US/English
External Power Bar
Select model: None/Feature disabled
Should all users, or only the admin user be able to control power to attached systems?
Normal (admin only)
Keyboard Mapping (for localization)
In many parts of the world, the keyboard has extra keys and/or different layout to better suit the local language than the default US/English layout. If your host O/S is expecting a keyboard of a special type, choose it here.
If the wrong value is used here, special language keys will not work, and some basic symbols (such as ") may not work correctly. The key layout of the "remote" keyboard must match the key layout of the "local" keyboard defined here.
External Power Bar
Connect a remote power control device to the serial port, and choose the model from the list below. You will typically require a straight-thru 9-pin cable to connect between this device and the power bar.
Once enabled, a status and control area will appear on the home page. Individual ports can then be controlled and monitored.
Applet VncViewer started

Keyboard Mapping

In many parts of the world, the keyboard has extra keys and/or different layout to better suit the local language than the default US/English layout. If your host O/S is expecting a keyboard of a special type, choose it here.

If the wrong value is used here, special language keys will not work, and some basic symbols (such as “) may not even work correctly. The key layout of the “remote” keyboard must match the key layout of the “local” keyboard defined here.

External Power Bar

Connect a remote power control device to the serial port, and choose the model from the list. You must use the “front” serial port (DTE pin out). The rear port is reserved for setup and IPMI functions. A straight-thru cable is typically required.

Once enabled, a status and control window will appear, individual ports can then be power controlled and monitored.

IX. How to Setup the SNMP Agent and Configuration

Please click on **SNMP** to get the following image.

Communities

Read-only Community

This community is allowed to read any value and is not allowed to write or change anything. To disable read access, set this string to nothing (empty). The default value is **public**.

Read-write Community

This community is allowed to read and change any value. You should make this value unique and keep it confidential for security reasons: anyone who knows this string can control this device and all systems attached to it. Leave this string empty to disable SNMP write access.

Agent Identification

Location

This string is sent as the **system.sysLocation** value. It should describe the location of this device.

Contact Name

This string is sent as the **system.sysContact** value. It should describe who to contact regarding this machine. Typically it includes an email address.

Traps

Trap/Inform Community

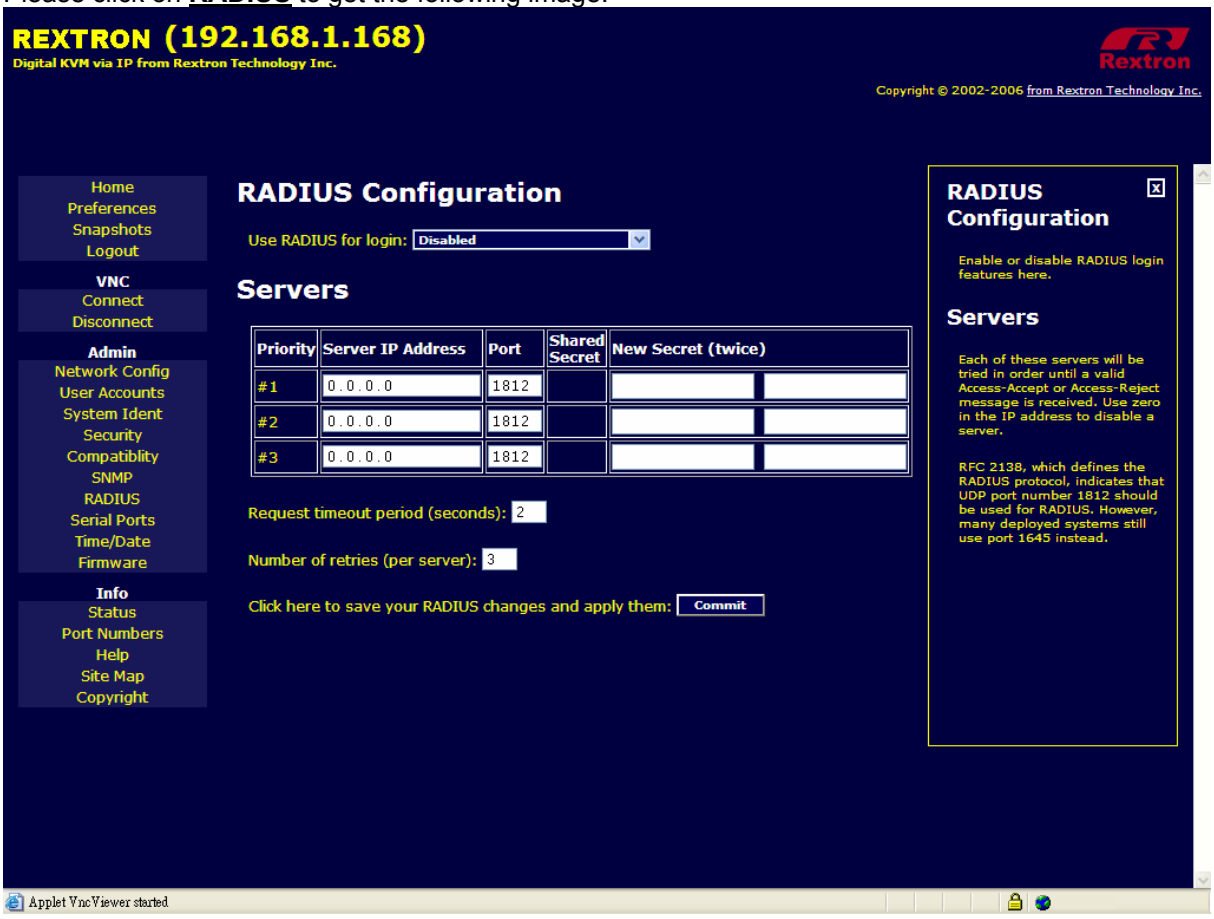
When trap messages are sent, they are sent using this community. This should be a community that exists on your trap server.

Trap Sink 1 (primary)

This host will be the target for any traps/inform messages sent. These address must be specified numerically. Leave blank if not needed.

X. How to Setup RADIUS authentication

Please click on **RADIUS** to get the following image.



The RADIUS server requires the IP address, the UDP port number (1812 - *default* or 1645) and the shared secret. The shared secret is used to encrypt communications and corresponds to a shared password for the RADIUS server and the client machine. Two additional servers may be defined for backup purposes. Each server will be tried in order, using the indicated number of retries and timeout period, which are configurable on the same page. *Remember to enable RADIUS after configuring it*.

While RADIUS authentication is enabled, the locally defined accounts on the KVM control over IP module will not be used, except for the SSH login. However, if a user name of the form “name.local” is given at the RADIUS prompt, the system will use “name”; check the password locally, and skip RADIUS authentication. Delete all local accounts to avoid this behavior. When connecting via VNC, a login screen is generated that asks for a RADIUS username and password.

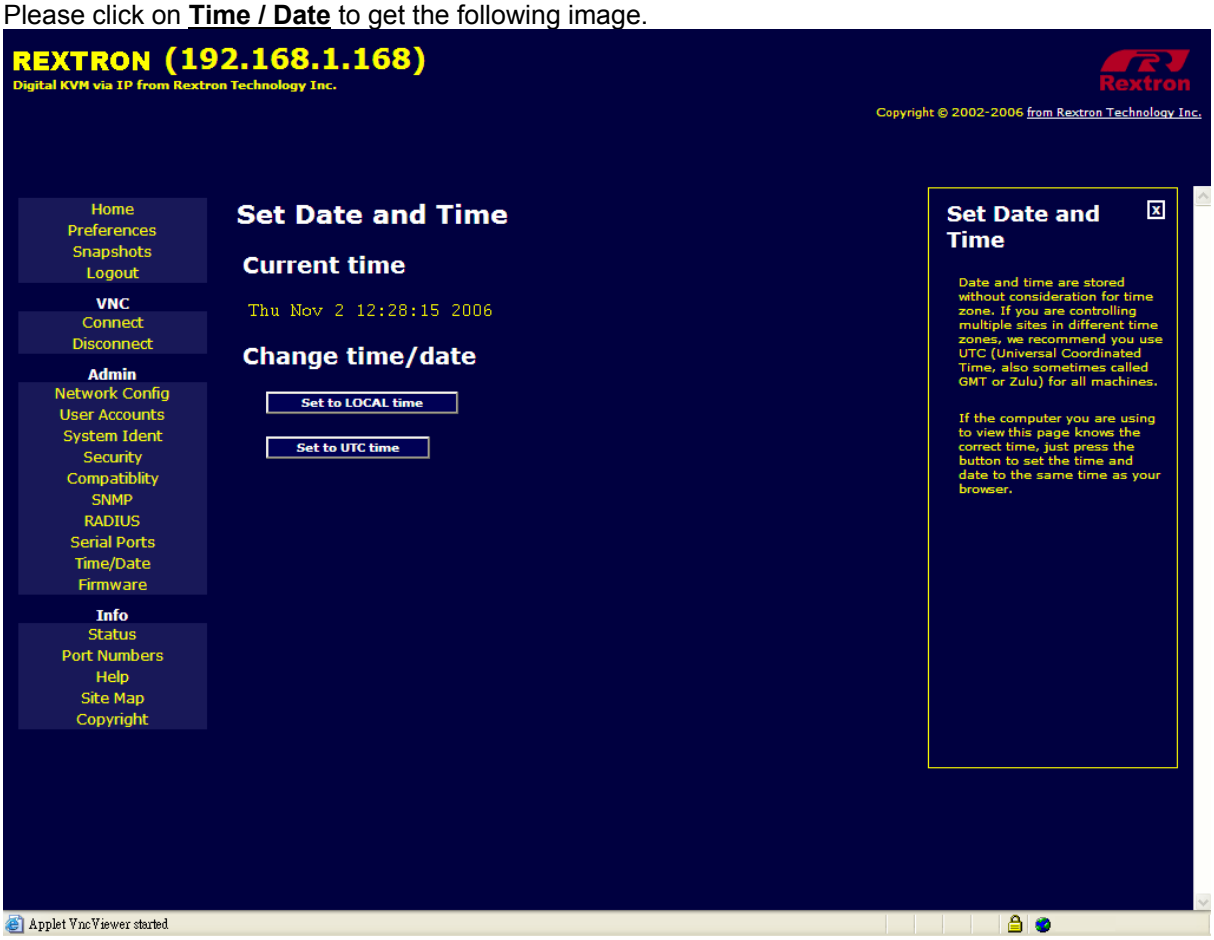
XI. How to Setup and Control the External Serial Consoles

Please click on **Serial Ports** to get the following image.

There are two ways that **Digital KVM via IP** can control the serial devices such as power bar, router, printer, and so on. The first way is connect the serial devices with the DTE serial port or DCE serial port of **Digital KVM via IP**, and the second way is connect the serial devices with the serial port of **Serial Supervisor**. For more information, refers to Appendix **G.**

XII. How to Set Date and Time

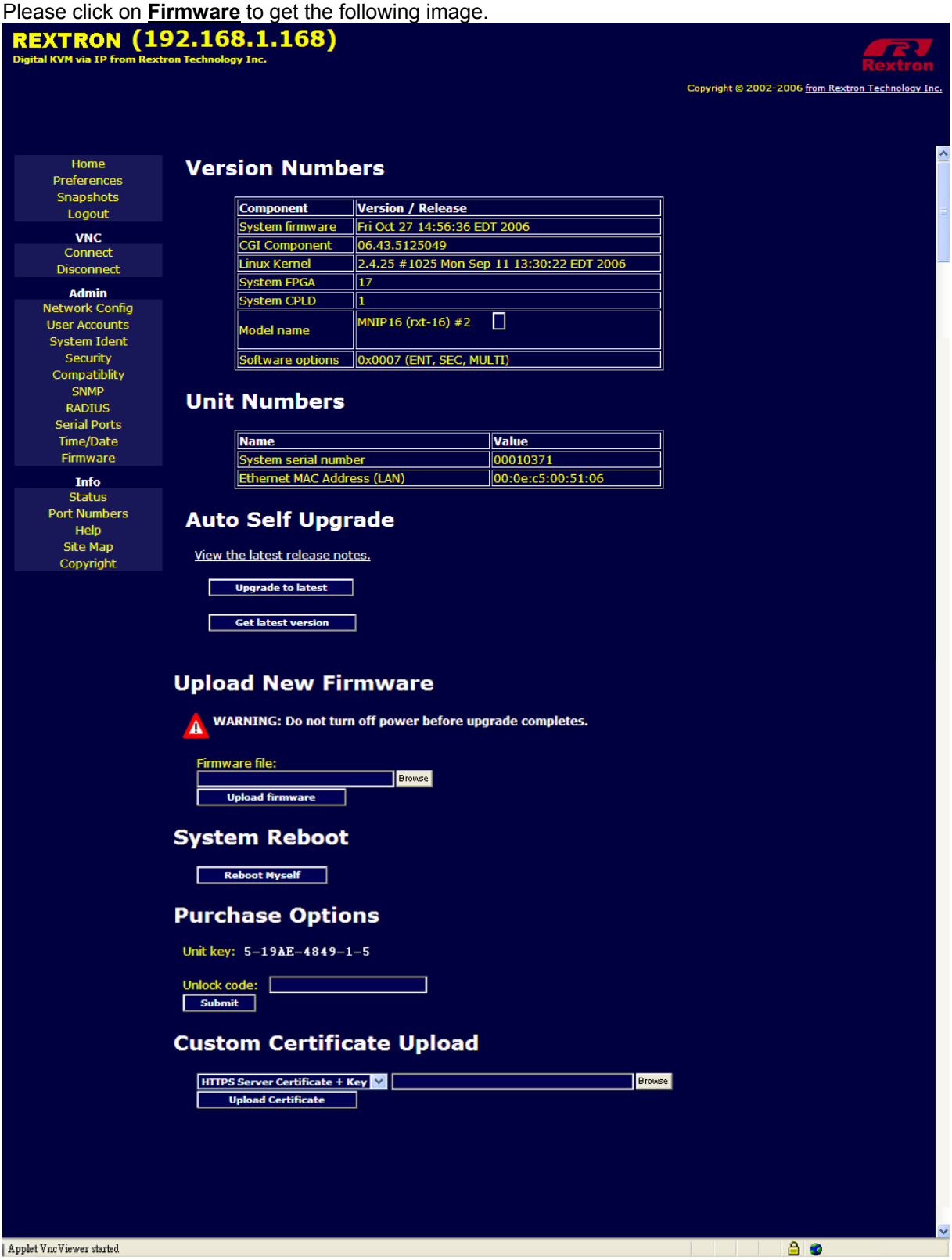
Please click on **Time / Date** to get the following image.



Allow you to set your **Digital KVM via IP** to **Local Time** or **Universal Coordinated Time** (GMT). Date and time is stored without consideration for time zone. If you are controlling multiple sites in different time zones, we recommend you use GMT for all machine.

XIII. How to Update your Firmware

Please click on **Firmware** to get the following image.



The firmware of **Digital KVM via IP** is online upgradeable, upgrading to the latest version, please login as admin. That is, only the administrator has rights to do so.

Auto Self Upgrade
The **Digital KVM via IP** includes an innovative feature allowing the unit to upgrade itself over the Internet. Simply click on the button labeled "**Upgrade to Latest**" and the unit will go out to the Internet and download the latest version of the system firmware and then install it. If the unit cannot access the Internet directly (perhaps due to a web proxy or other firewalls), then a page will be shown that causes your browser to download the required file. Save this file to disk and then upload it as described in the next section, Manual Upload. The main FPGA is upgraded separately, and has its own Get latest button. This file is unique for each unit, so it must be done in this manner.
If you have multiple units to upgrade, you may choose the "**Get latest version**" button that will not attempt to upgrade the unit directly, but will instead fetch the required file. This file can be uploaded to multiple units manually.

Manual Upload
Enter the name of the firmware file that you received from **Rextron Technology Inc.** into the field provided (or use the Browse... button). Press Start Upload and wait until a successful upload message is shown.

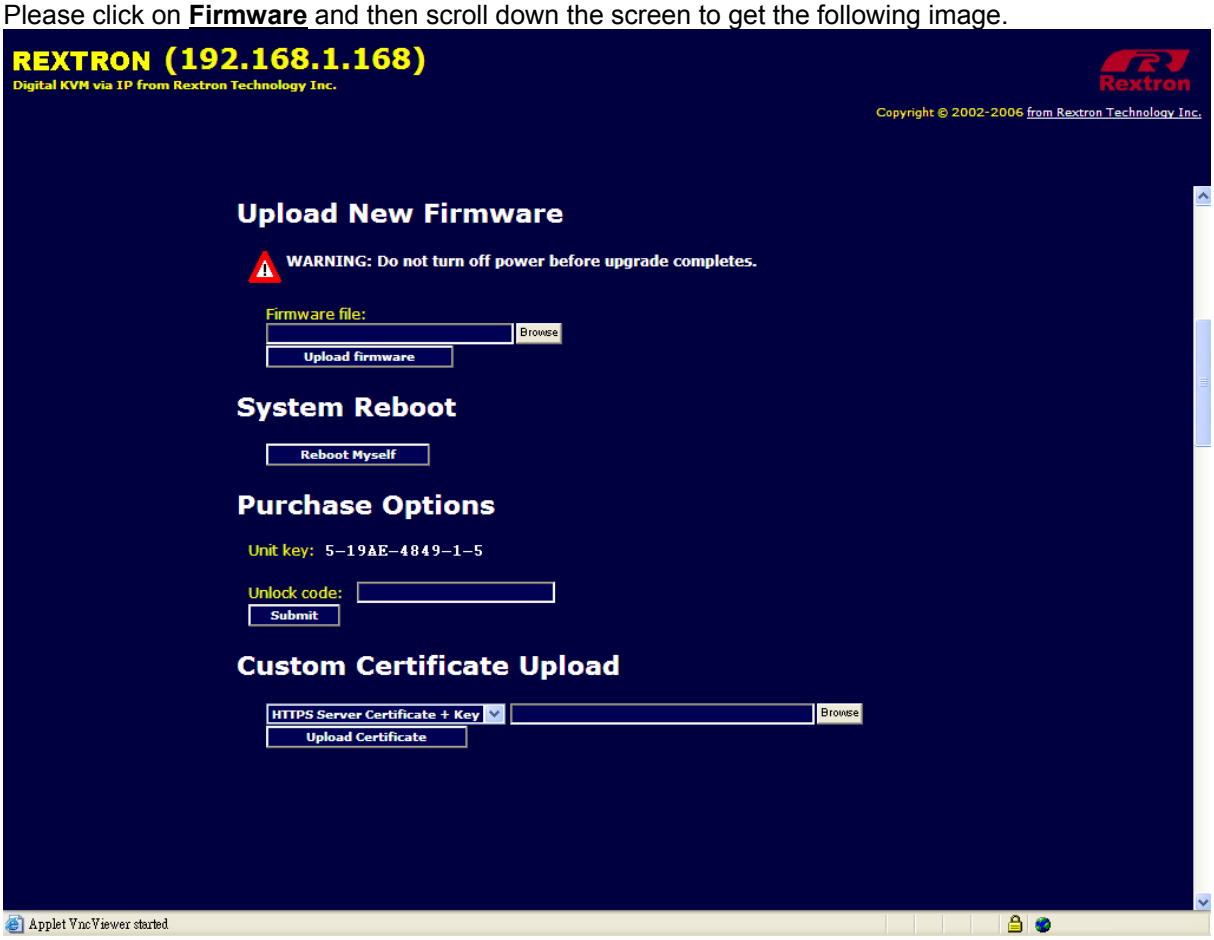
NOTE: Remember the following during the firmware upgrade…

- Do NOT turn off power to unit before this operation completes successfully. It may take several minutes to write to flash memory.
- The unit will sometimes reboot as part of the upgrade procedure, depending on which system component is upgraded. You will have to reconnect and re-login in those cases.
- Wait at least two minutes after pressing Start. Do not assume the upload did not work. There is no status indicator bar to show the progress of the upload. The upload could simply be slow.
- Each file that is distributed upgrades a different component of the system. Therefore, be sure to apply all files you are given as part of an upgrade. The system knows what to do with each file you give it, and they are checked for validity before being applied.

System Reboot
After installing new firmware, you may want to reboot.

XIV. How to Upload Custom Certificate

Please click on **Firmware** and then scroll down the screen to get the following image.



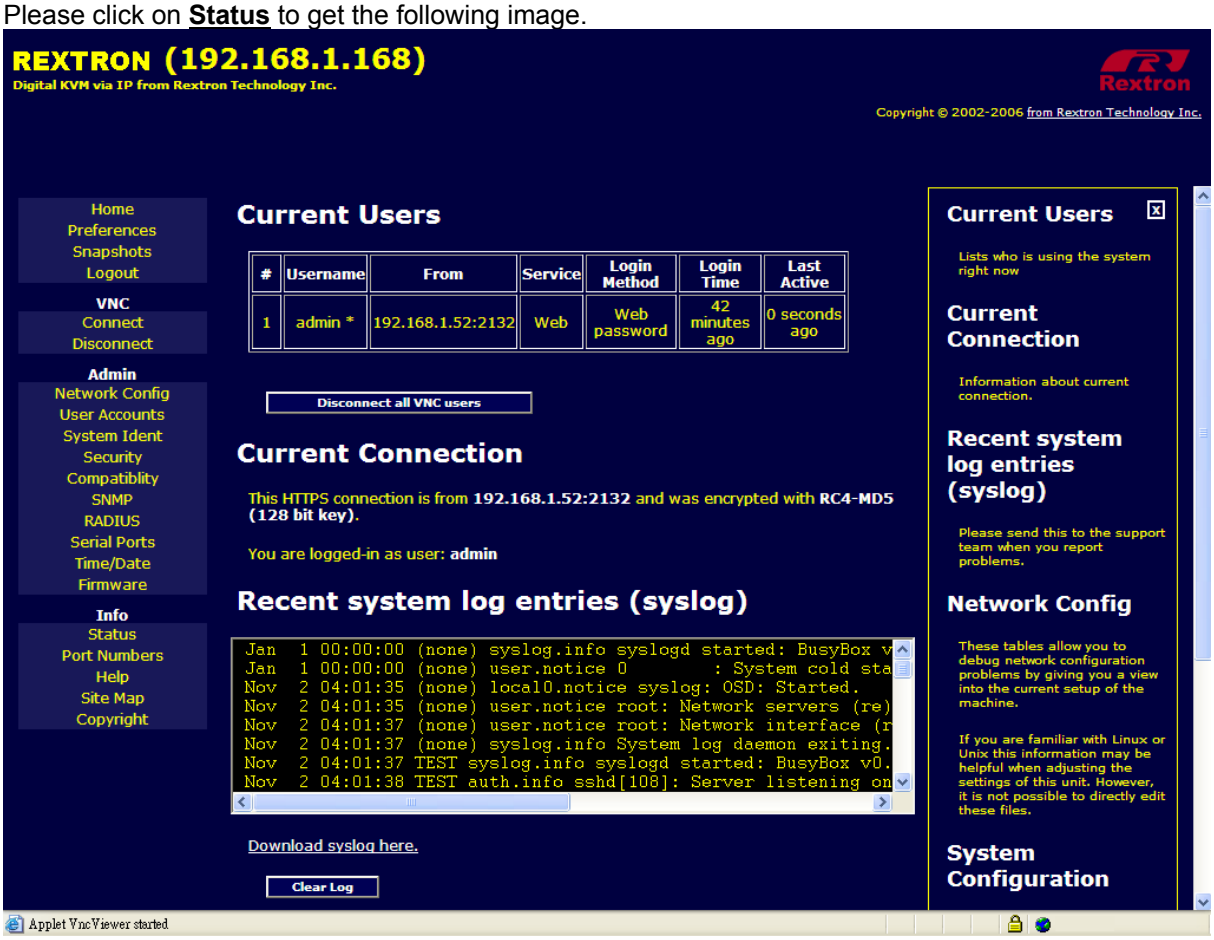
Upload your own certificate to replace the factory-supplied SSL certificate here.
We require an RSA private key and corresponding public certificate to be combined together into one PEM file. There should be no encryption on the private key and it must be first in the file. Therefore, we expect a text file in this format:

-----BEGIN RSA PRIVATE KEY-----
[based64 encoded key]
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
[based64 encoded certificate]
-----END CERTIFICATE-----
[end of file]

Uploading the root CA public certificate is optional and only affects the link on the login page. It does not affect operation otherwise. It is just a X.509 PEM file holding a public certificate.

XV. How to Lookup your Digital KVM via IP System Status

Please click on **Status** to get the following image.

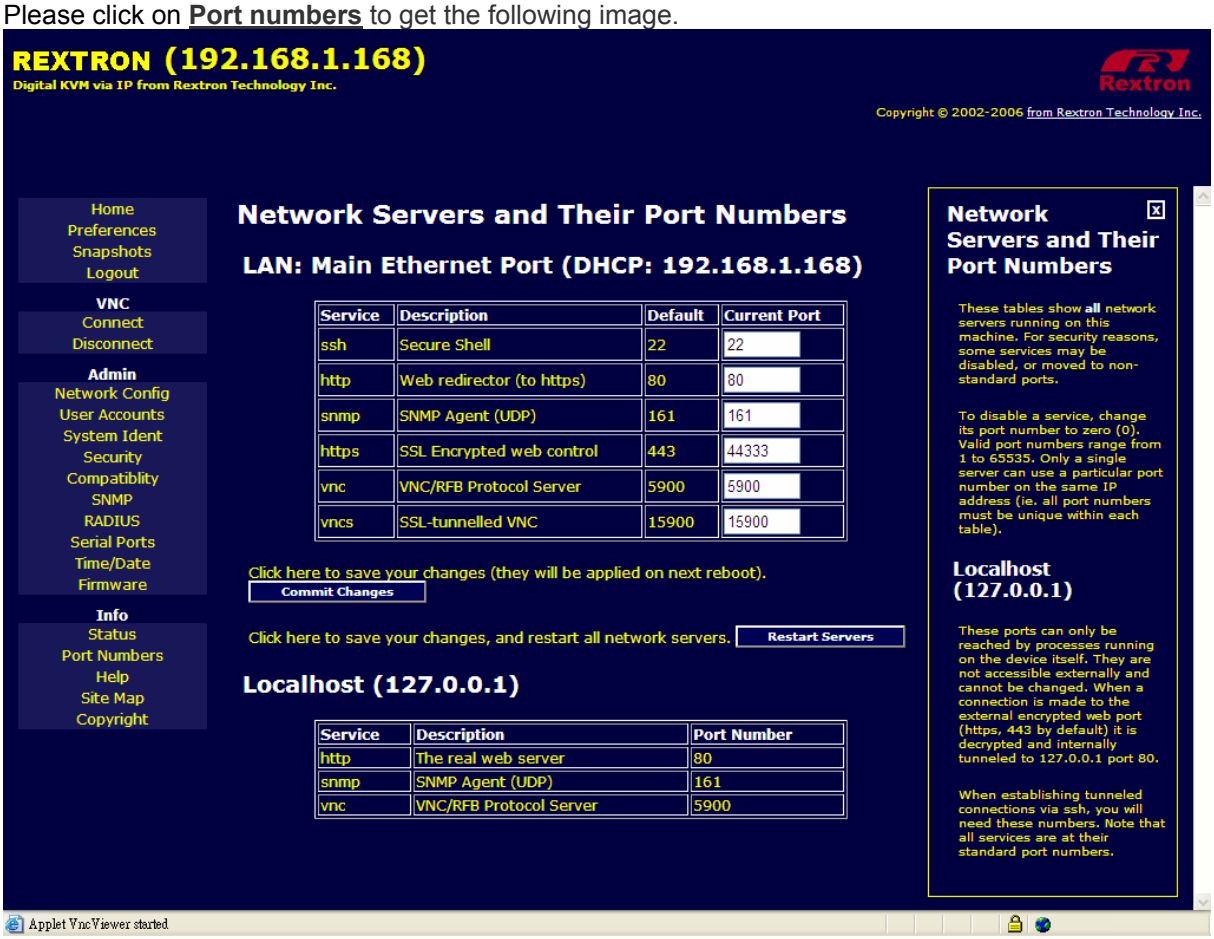

REXTRON (192.168.1.168)
Digital KVM via IP from Rextron Technology Inc.
Rextron
Copyright © 2002-2006 from Rextron Technology Inc.
Home
Preferences
Snapshots
Logout
VNC
Connect
Disconnect
Admin
Network Config
User Accounts
System Ident
Security
Compatiblity
SNMP
RADIUS
Serial Ports
Time/Date
Firmware
Info
Status
Port Numbers
Help
Site Map
Copyright
Current Users
Username From Service Login Method Login Time Last Active
1 admin * 192.168.1.52:2132 Web Web password 42 minutes ago 0 seconds ago
Disconnect all VNC users
Current Connection
This HTTPS connection is from 192.168.1.52:2132 and was encrypted with RC4-MD5 (128 bit key).
You are logged-in as user: admin
Recent system log entries (syslog)
Jan 1 00:00:00 (none) syslog.info syslogd started: BusyBox v
Jan 1 00:00:00 (none) user.notice 0 : System cold sta
Nov 2 04:01:35 (none) local0.notice syslog: OSD: Started.
Nov 2 04:01:35 (none) user.notice root: Network servers (re)
Nov 2 04:01:37 (none) user.notice root: Network interface (r
Nov 2 04:01:37 (none) syslog.info System log daemon exiting.
Nov 2 04:01:37 TEST syslog.info syslogd started: BusyBox v0.
Nov 2 04:01:38 TEST auth.info sshd[108]: Server listening on
Download syslog here.
Clear Log
Current Users
Lists who is using the system right now
Current Connection
Information about current connection.
Recent system log entries (syslog)
Please send this to the support team when you report problems.
Network Config
These tables allow you to debug network configuration problems by giving you a view into the current setup of the machine.
If you are familiar with Linux or Unix this information may be helpful when adjusting the settings of this unit. However, it is not possible to directly edit these files.
System Configuration
Applet VncViewer started

This menu shows your **Digital KVM via IP** system status as following:

- **Recent System Log**: it records every log entry, including what time the user log in, what identification the user log in, and so forth.
- **Current Users**: it shows the users' list that currently log in.
- **Current Connection**: it shows the current IP and what encryption you are using to log in **Digital KVM via IP**.
- **Network Config**: these tables allow you to debug network configuration problems by giving you a view into the current setup of machine.
- **Disconnect all VNC users**: in case of the users are locked-out of the system because someone has left a VNC session connected and cannot be reached through other means, the admin user can close all VNC connections.

XVI. How to Setup Port Number

Please click on **Port numbers** to get the following image.


REXTRON (192.168.1.168)
Digital KVM via IP from Rextron Technology Inc.
Rextron
Copyright © 2002-2006 from Rextron Technology Inc.
Home
Preferences
Snapshots
Logout
VNC
Connect
Disconnect
Admin
Network Config
User Accounts
System Ident
Security
Compatiblity
SNMP
RADIUS
Serial Ports
Time/Date
Firmware
Info
Status
Port Numbers
Help
Site Map
Copyright
Network Servers and Their Port Numbers
LAN: Main Ethernet Port (DHCP: 192.168.1.168)
Service | Description | Default | Current Port
ssh | Secure Shell | 22 | 22
http | Web redirector (to https) | 80 | 80
snmp | SNMP Agent (UDP) | 161 | 161
https | SSL Encrypted web control | 443 | 44333
vnc | VNC/RFB Protocol Server | 5900 | 5900
vncs | SSL-tunnelled VNC | 15900 | 15900
Click here to save your changes (they will be applied on next reboot).
Commit Changes
Click here to save your changes, and restart all network servers.
Restart Servers
Localhost (127.0.0.1)
Service | Description | Port Number
http | The real web server | 80
snmp | SNMP Agent (UDP) | 161
vnc | VNC/RFB Protocol Server | 5900
Network Servers and Their Port Numbers
These tables show all network servers running on this machine. For security reasons, some services may be disabled, or moved to non-standard ports.
To disable a service, change its port number to zero (0). Valid port numbers range from 1 to 65535. Only a single server can use a particular port number on the same IP address (ie. all port numbers must be unique within each table).
Localhost (127.0.0.1)
These ports can only be reached by processes running on the device itself. They are not accessible externally and cannot be changed. When a connection is made to the external encrypted web port (https, 443 by default) it is decrypted and internally tunneled to 127.0.0.1 port 80.
When establishing tunneled connections via ssh, you will need these numbers. Note that all services are at their standard port numbers.
Applet VncViewer started

This menu shows all network servers running on this machine. For the security reasons, some services may be disabled, or moved to non-standard ports.

XVII. How to Speed Up your Digital KVM via IP

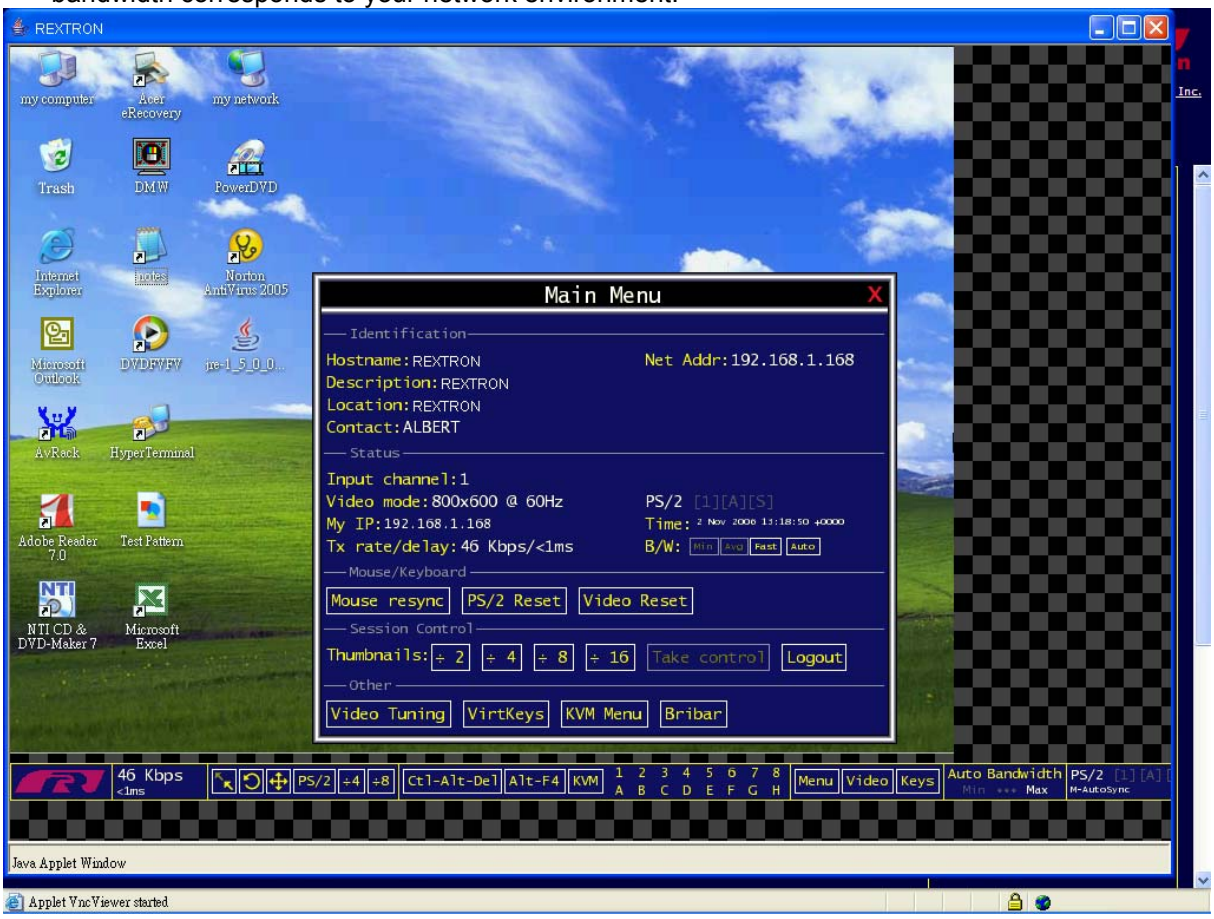
There are 2 ways to speed up the VNC screen connection.

1. Please click on Preferences to get the following image.

REXTRON (192.168.1.168)
Digital KVM via IP from Rextron Technology Inc.
Rextron
Copyright © 2002-2006 from Rextron Technology Inc.
Home
Preferences
Snapshots
Logout
VNC
Connect
Disconnect
Admin
Network Config
User Accounts
System Ident
Security
Compatiblity
SNMP
RADIUS
Serial Ports
Time/Date
Firmware
Info
Status
Port Numbers
Help
Site Map
Copyright
User preferences
Open VNC connection immediately on web login
No (use buttons to start VNC)
Yes (VNC started on login)
Force bandwidth mode
Auto (not forced)
Min (slowest/least traffic)
Average
Max (fastest/most traffic)
Reduce network traffic by limiting colors
8-bit (256 colors)
12-bit (4096 colors)
16-bit (default: 65536 colors)
VNC Callback instead of Java VNC
No (use Java client)
Yes (use VNC callback to native client)
Encrypt VNC connection
Encrypt over Internet only
Always Encrypt
Never Encrypt
Optimize for full-screen VNC
No (normal)
Yes (don't show Bribar)
Skip welcome window on VNC connection
No (normal)
Yes (skip welcome window)
Save Changes
Default Values
Reset all
User preferences
Your current user preferences are listed here. You may change any of them and save with the button below.
Most of these preferences affect how the VNC client and server interact.
Open VNC connection immediately on web login
Start a VNC connection immediately after login to the web server. The connect button does not need to be used.
Force bandwidth mode
By default, the initial connection performance (RTT) is measured and used to select whether to optimize a high bandwidth connection or low. If the connection improves, the bandwidth used will be adjusted. You can override this while the connection is operating. Use this preference to override auto mode and force the B/W mode.
Reduce network traffic by limiting colors
Network traffic (bandwidth) may be reduced by reducing the image quality. We do not recommend 12-bit mode but provide it here as a middle ground.
VNC Callback instead of Java VNC
If you have a VNC client 'listening' on your work station and would prefer to use that instead of Java client, enable this option.
Encrypt VNC connection
By default we will use the cleartext (not encrypted) connection when the network connection looks like a 'local link' (ie. same IP subnet). Encrypted mode is the default on Internet connections. Use this control to force the use of the encrypted VNC connection or no encryption. Only affects Java VNC client.
Optimize for full-screen VNC
This control hides the Bribar
java.lang.NullPointerException

From “Force bandwidth mode”, you can select the proper bandwidth corresponds to your network environment. Generally speaking, it’s recommended to select “Max” for the LAN users and “Min” for the WAN users.
From this screen, you can do the bandwidth control. There are 4 modes available: Min, Avg, Max, and Auto. If you choose Min/Avg/Max then you will override the default, Auto. As the automatic mode measures actual network performance, you may see the current mode switch from Min up to Avg or Max. The different modes indicate more time spent on compression versus more bandwidth. There is no visual difference between the modes, but there can be a noticeable difference in speed and smoothness.

2. Please click on “VNC Connect”, you’ll get the VNC screen. That is, you will see the screen of the host computer(s), please scroll the screen to the bottom. It is the Bribar (refers to Chapter 5, section C: How to Use the Bribar) down there, please click on Menu (refers to Chapter 5, section D: How to Use the Main Menu). Should you find “B/W” on the screen, click the proper bandwidth corresponds to your network environment.



From this screen, you can do the bandwidth control. There are 4 modes available: Min, Avg, Max, and Auto. The white button is the mode the system is currently operating. If you choose Min/Avg/Max then you will override the default, Auto. As the automatic mode measures actual network performance, you may see the current mode switch from Min up to Avg or Max. The different modes indicate more time spent on compression versus more bandwidth. There is no visual difference between the modes, but there can be a noticeable difference in speed and smoothness.

NOTE: **You may need to upgrade or download your Java (http://www.java.com) support in your browser before using the VNC screen to remote control the host computer(s); however, most modern browsers come with a version of Java that is compatible with this application.**

■ Chapter 4 Accessing KVM Features

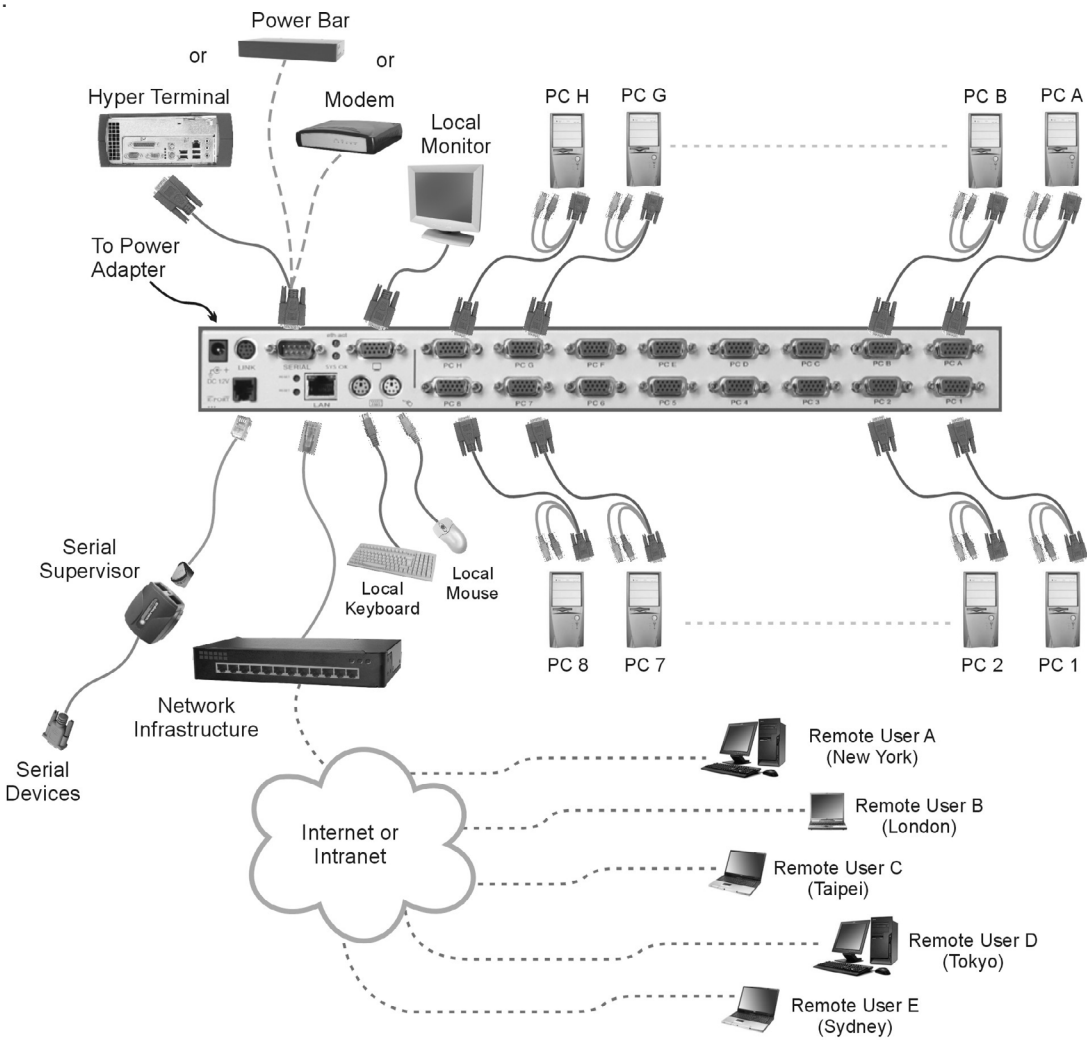
(For ALL models except MNIP01 , WMM001 and WUM001)

Once you can access and configure the networking component of the **Digital KVM via IP**, you can use it to select and control the managed computers connected to it. This section describes how to add additional KVM switches to the master unit for greater flexibility, and how to use the KVM on-screen display (KVM-OSD) system to manage your computers. Once you have established a VNC session with the **Digital KVM via IP**, you can access the KVM features as though you were at a local console.

A. Cascade Configuration

You can connect a second level of KVMs to one or more of your **Digital KVM via IP**'s **PC 1~8** ports. The KVM switches connected to the **Digital KVM via IP** (the "Master switch") are known as Slaves. Once connected, the units will automatically configure themselves as either Masters or Slaves. You can only connect an equal or "smaller" KVM to the Master: a 16-port Master switch can have both 16-port and 8-port slave KVMs, an 8 port Master switch can have 8-port and 4-port Slaves, and so on.

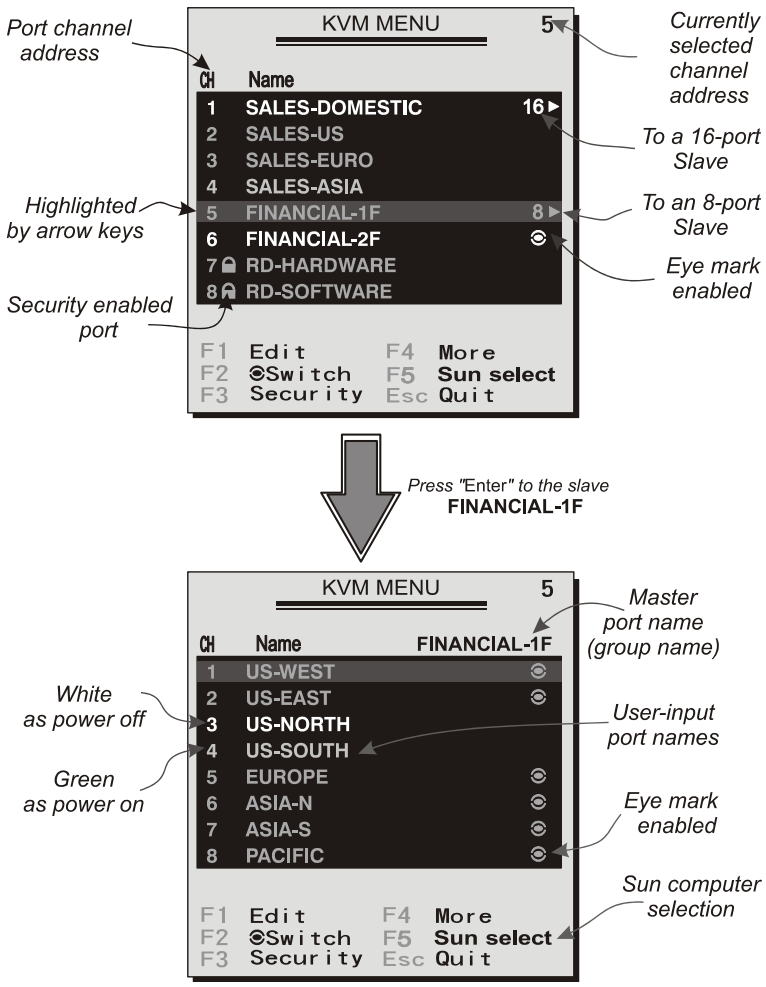
For example, the 16-port unit can support 136 computers, with 8 units of 16-port Slave KVMs, each connected to 16 computers. The Slave KVMs must be connected to the **PC 1~8** ports, not the **PC A~H** ports.



To cascade your KVMs, use a 1-to-3 PS/2 KVM cable to connect one of your Master switch's **PC 1-8** ports to the Slave KVM's **console port**. When turning on your cascaded switches, turn on the Master switch before turning on any of the others.

B. KVM-OSD Operations

(For ALL models except MNIP01 , WMM001 and WUM001)



KVM-OSD screen illustration

- ***UNIP04 / 08 / 16, WUM108D / 116D*** *models offer "**F5**", see Function key* ***F5***
- ***MNIP04 / 08 / 16, WMM108D / 116D*** *models do not offer "**F5**" function*

By hitting the *left* ***Ctrl*** key twice within two seconds, you may see the '**Hotkey Menu**' if it is enabled (a KVM-OSD option). Or, by hitting the *left* ***Ctrl*** key three times within two seconds, you will see a '**KVM MENU**' screen showing a list of the computers with corresponding port numbers, names, and statuses, see Figure 10.

The port number of the currently selected computer is displayed in red, same as the front indicator, at the upper-right corner of the KVM-OSD menu.

The color of a device name is green if it has power and is ready for operation, or, the white color means it has no power. KVM-OSD menu updates the color when it is activated. For 16-port models, pressing the ***PageUp*** and ***PageDown*** keys to view 8 other computers.

Using the " (", " (", " 1 " ~ " 8 " or " A " ~ " H " to highlight a computer and using the ***Enter*** key to select it. Or, you may press ***Esc*** to exit KVM-OSD and remove it from the display; the status window returns to the display and indicates the currently selected computer or operating status.

A triangle mark (▸) to the right of a name indicates the port is cascaded to a Slave; the number at the left of the triangle mark shows the number of ports the Slave has, i.e. **8** ▸ for an 8-port Switch. ***Enter*** key brings you one level down and another screen pops up listing the names of the computers on that Slave. The name of the Slave will be shown at the upper right corner of the KVM-OSD menu. It is useful to group computers and still be able to see the group name.

An eye mark (👁) on the right of a name indicates that computer is selected and monitored in Scan mode. In the KVM-OSD, this mark can be switched on or off by function key ***F2***.

Press ***Esc*** key to exit the KVM-OSD and to return to the selected computer; the computer name is also shown on the screen.

- Function key ***F1*** : To edit name entry of a computer or a Slave with up to 14 characters. First, highlight a port then press ***F1*** followed by name entry. Valid characters are 'A'~'Z', '0'~'9', and the dash character. Lowercase letters are converted to uppercase ones. Press ***Backspace*** to delete a letter one at a time. Non-volatile memory stores all name entries until you change, even if the unit is powered down.

- Function key ***F2*** : To switch the eye mark (👁) of a computer on or off. First, use the ↑ and ↓ arrow keys to highlight it, then press ***F2*** to switch its eye mark on or off. If *Scan Type* is '**Ready PC +👁**', only the power-on and eye mark selected computers will be displayed sequentially in Scan mode.

- Function key ***F3*** : To lock a computer from unauthorized access. To lock a device, highlight it then press ***F3***. Now, enter up to 4 **characters** ('A'~'Z', '0'~'9, '-') followed by ***Enter*** as a new password. A Security-enabled device is marked with a **lock** (🔒) following its port number. To *permanently* disable the security function from a locked device, highlight it, press ***F3*** then enter the password.

  If you want to access the locked device *temporarily*, simply highlight it and press ***Enter***, the KVM-OSD will ask you for the password. After entering the correct password, you are allowed to use the device. This device is automatically re-locked once you switch to another port. During Scan mode, the KVM-OSD skips the password-protected devices.

- Function key ***F4*** : More functions are available by hitting ***F4***. A new screen pops up displaying more functions as described below. Most of them are marked with a triangle (▸) indicating there are options to choose from. Using arrow key " ↑ ", " ↓ " to select the functions, and then press ***Enter***. Available options will be shown in the middle of the screen. Again, using arrow keys " ↑ ", " ↓ " to view options, and then press ***Enter*** to select it. You can press ***Esc*** to exit at any time.

  - *Auto Scan*

    In this mode, the KVM switch automatically switches from one power-on computer to the next sequentially in a fixed interval. During *Auto Scan* mode, the KVM-OSD displays the name of the selected computer. When *Auto Scan* detects any keyboard or mouse activity, it suspends the scanning till activity stops; it then resumes with the next computer in sequence. To abort the

Auto Scan mode, press the *left* **Ctrl** twice, or, press any front button. *Scan Type* and *Scan Rate* set the scan pattern. *Scan Type* (**F4** : More\Scan Type) determines if scanned computers must also be eye mark selected. *Scan Rate* (**F4** : More\Scan Rate) sets the display interval when a computer is selected before selecting the next one.

■ *Manual Scan*

Scan through power-on computers one by one by the keyboard control. You can type (**F4** : More\Scan Type) to determine if scanned computers must also be eye mark selected. Press the up arrow key " ↑ " to select the previous computer and the down arrow key " ↓ " to select the next computer. Press any other key to abort the Manual Scan mode.

■ *Audio Stick*

An optional multimedia module can be **LINK**ed to the back of each KVM Switch for selecting microphone and stereo speaker signals. There are two options for *Audio Stick*: **On** and **Off**. When set to '**On**', audio selection follows computer selection. When set to '**Off**', audio selection stops following computer selection. It is useful if you want to listen to a particular computer's audio signal while operating other computers. The non-volatile memory stores the *Audio Stick* setting.

■ *Scan Type*

Ready PC +👁: In Scan mode, scan through power-on and eye mark selected computers.

Ready PC: In Scan mode, scan through power-on computers.

👁 **Only**: In Scan mode, scan through any 👁 selected computer regardless of computer power status. The non-volatile memory stores the *Scan Type* setting.

■ *Scan Rate*

Sets the duration of a computer displayed in *Auto Scan* mode. The options are **3** seconds**, 8** seconds**, 15** seconds**,** and **30** seconds. The non-volatile memory stores the *Scan Rate* setting.

■ *Keyboard Speed*

Digital KVM via IP offers keyboard typematic setting that overrides the similar settings in BIOS and in Windows. Available speed options are **Low**, **Middle**, **Fast** and **Faster** as 10, 15, 20 and 30 characters/sec respectively. The non-volatile memory stores the Keyboard Speed setting.

■ *Hotkey Menu*

When you hit the *left* **Ctrl** key twice within two seconds, the "Hotkey Menu" appears displaying a list of hotkey commands if the option is **On**. The 'Hotkey Menu' can be turned **Off** if you prefer not to see it when the *left* **Ctrl** key is hit twice. The non-volatile memory stores the Hotkey Menu setting.

■ *CH Display*

Auto Off: After you select a computer, the port number and name of the computer will appear on the screen for 3 seconds then disappear automatically. **Always On**: The port number and name of a selected computer and/or KVM-OSD status displayed on the screen all the time. The non-volatile memory stores the CH Display setting.

■ *Position*

The position of the selected computer and/or IP-OSD status displays on screen during the operation. The actual display position shifts due to different VGA resolution, the higher the resolution the higher the displayed position. The non-volatile memory stores the Position setting.

Upper Left, **Upper Right**,
Lower Left, **Lower Right,**

Middle.

■ *Country Code for Sun* ***(For UNIP04 / 08 / 16, WUM108D / 116D only***)
Sun keyboards of different languages have different layouts. The KVM switch is able to emulate a Sun keyboard for a specific language type or country such as **Arabic**, **Belgian**, **US**, **Yugoslavia**, **and so forth**. Select the proper country code that matches ***ALL*** of your Sun computers.

■ *Max. Resolution* ***(For UNIP04 / 08 / 16, WUM108D / 116D only***)
You can adjust the monitor resolution under this sub-menu. There are the following selections: 1024*768, 1280*1024,1600*1200,1920*1440, and "DDC2B Disable".

● Function key ***F5*** : ***(For UNIP04 / 08 / 16, WUM108D / 116D only***) To switch the **Sun** mark of a port on or off indicating the computer is a Sun server. Sun servers have more keys on the keyboard than a PC. When a **Sun-**marked port is selected, the KVM Switch starts to translate the keys from a PS/2 keyboard to a Sun keyboard. See *Sun Keyboard Mapping* for detail.

● ***Esc*** : To exit the KVM-OSD, press the ***Esc*** key.

C. Hot Key Commands

A hot key command is a short keyboard sequence to select a computer, activate a computer scan, etc. A hot-key sequence starts with two Left Control keystrokes followed by one or two more keystrokes.

The short form hot-key menu can be turned on as an KVM-OSD function (***F4*** : More\Hotkey Menu) every time the left ***Ctrl*** key is pressed twice.

Left Ctrl refers to the ***Ctrl*** key located at the left side of the keyboard.
1~8/A~H refer to the number keys 1 to 8 at the upper row of the keyboard (Do not use the keypad at the right of the keyboard) and character keys A to H (case insensitive).

■ *Selecting a Computer*
To select a computer by hot-key command you need to know the device's channel address, which is determined by the KVM connection. For a computer connected to the Master switch, the address is represented by the PC port number (**1~8**/**A~H**). For example, to access the PC plugged into port 7 of the Master switch, type:

left ***Ctrl*** + left ***Ctrl*** + ***7***

For a computer connected to a Slave KVM, you need to know the channel address of the Slave unit (**1~8**) and then the channel address of the device (**1~8**/**A~H**). (Please note that only Master's **PC 1~8** ports can be connected to a Slave.) For example, to access the computer plugged into **console port** of a Slave KVM that is plugged into Port 6 of the Master switch, type:

left ***Ctrl*** + left ***Ctrl*** + ***6*** + ***C***

■ *Auto Scan*
Auto Scan automatically scans through powered computers at a fixed interval:

left ***Ctrl*** + left ***Ctrl*** + ***F1***

When Auto Scan detects any keyboard or mouse activity, it suspends the scanning until activity stops; it then resumes with the next computer in sequence. The length of the Auto Scan interval (Scan Rate) is adjustable (see **Scan Rate** on the following page). To abort the Auto Scan mode, press the left Ctrl key twice.

NOTE: The **Scan Type** setting will determine whether computers must be eye-marked to be included in the scan. See page 27 for details.

■ *Manual Scan*

Manual Scan enables you to manually switch back and forth between powered computers:

left ***Ctrl*** + left ***Ctrl*** + ***F2***

Press the up or down arrow to select the previous or next computer in sequence. Press any other key to abort the Manual Scan.

NOTE: The **Scan Type** setting will determine whether computers must be eye-marked to be included in the scan. See page 27 for details.

■ *Scan Rate*

Scan Rate sets the duration between switching to the next computer in Auto Scan mode:

left ***Ctrl*** + left ***Ctrl*** + ***F3***

The unit switches between scan intervals of **3**, **8**, **15** and **30** seconds.

■ *Keyboard Typematic Rate*

You can adjust the **keyboard typematic rate** (given in characters/sec). This setting over-rides the **keyboard typematic rate** of your BIOS and any operating system.

left ***Ctrl*** + left ***Ctrl*** + ***F4***

The unit switches between rates of **10**, **15**, **20** and **30** characters/sec.

■ *Audio Stick*

A multimedia module can be LINKed to the back of the Master switch for selecting microphone and stereo speaker signals. There are two options for Audio Stick: On and Off. When set to On, audio selection follows computer selection. When set to Off, audio selection stops following computer selection. It is useful if you want to listen to a particular computer's audio signal while operating other computers.

left ***Ctrl*** + left ***Ctrl*** + ***F5***

(**NOTE:** This is an **optional** feature requiring a separate device to be connected to the Master switch.)

■ *Changing Your Configuration*

After the initial power up, any device (either a KVM or a PC) can be added or removed from any **PC x** port on the KVM without having to power down the Master switch. Make sure that devices are turned offer before connecting them to the Master switch.

NOTE: After changing your configuration, the KVM-OSD will automatically update to reflect the new configuration.

■ Chapter 5 How to Remotely Control the Host Computer(s)

A. Accessing the VNC Interface

There are three ways to communicate with the **Digital KVM via IP** in order to control the host computer(s).

I. **Web interface**: The integrated Web server includes a Java-based VNC client. This allows easy browser-based remote control.
II. **Native VNC client**: There are several third-party software programs that use the standard VNC protocol, available in open source and commercial VNC clients.
III. **SSH Tunnel**: By default, there is a standard SSH server running on port 22 (the standard SSH port). Once connected via SSH, the VNC traffic is tunneled through the SSH connection and encrypts the VNC session. Each method will be discussed briefly in the following section. The type of encryption method or client used is not critical.

I. Web Interface

The Java-based VNC client that is integrated into the **Digital KVM via IP** interface requires a browser with cookies and JavaScript enabled. To start the Java VNC client, login to the Web configuration interface and click on the thumbnail of the desktop on the Home menu, or follow one of the two links on that page:

Java VNC with no encryption (faster).
Java VNC with SSL encryption (more secure).

You may need to upgrade or download your Java (http://www.java.com) support in your browser before using the VNC screen to remote control the host computer(s); however, most modern browsers come with a version of Java that is compatible with this application.
The Java VNC client makes a connection back to the KVM control over IP module over port 5900 (by default) or 15900, if encrypted. The encrypted connection is a standard SSL (Secure Socket Layer) encrypted link that encrypts all data from the session, including the actual video pictures.

Because Java is considered a "safe" programming language, the Java VNC client has some limitations. Certain special keystrokes cannot be sent, such as "**Scroll Lock**" on the keyboard.

This client software requires the use of Java 2 (JRE 1.4) to enable features like wheel mouse support. Sun Microsystems's Java site, www.java.com, is an excellent resource to ensure your browser and operating system is up-to-date.

II. Native VNC Client

This system implements the VNC protocol, so any off the shelf VNC client can be used. There are over 17 different VNC clients available and they should all work with this system. This system automatically detects and makes use of certain extensions to the basic RFB protocol that is provided by the better VNC clients.

The best client currently is TightVNC (www.tightvnc.com). Binaries are available for Windows, Linux, MacOS and many versions of Unix. Source code for all clients is available there too. This version of VNC is being actively developed.

The authoritative version of VNC is available from RealVNC (www.realvnc.com). This source base is the original version of VNC, maintained by the original developers of the standard.

For a commercial, supported version of VNC, you should consider TridiaVNC (www.tridiavnc.com). Their version of VNC is a superset of TightVNC and contains a number of enhancements for use in a larger corporate environment.

NOTE: Some native VNC clients may require a flag or setting indicating they should use BGR233 encoding by default. If this flag is not set, you may see a garbled picture and the client will fail. The Unix versions of VNC require the flag -bgr233. For examples on using this flag, review the commands in the following section.

III. SSH Tunnel (with Native VNC client)

If you are using openssh, here is the appropriate Unix command to use, based on the default settings on a machine at 192.168.1.123:

```
ssh -f -l admin -L 15900:127.0.0.1:5900192.168.1.123 sleep 60
vncviewer -bgr233 127.0.0.1::15900
```

NOTEs: A copy of these commands, with appropriate values filled in for your current system setting, is provided in the *on-line help* page. This allows you to "cut-and-paste" the required commands accordingly.
You have 60 seconds to type the second command before the SSH connection will be terminated.
The port number "15900" is arbitrary in the above example and can be any number (1025...65535). It is the port number used on your client machine to connect your local SSH instance with the VNC client. If you want to tunnel two or more systems, you will need to use a unique number for each instance on the same SSH client machine.
Some Unix versions of the VNC client have integrated SSH tunneling support. Some clients require your local user id to be the same as the userid on the system.
Use a command like this: vncviewer -bgr233 -tunne**192.168.1.123**:22

B. Using the VNC Menu

One of the unique features of this product is the VNC menu system. Whenever you see a window with a dark blue background and grey edges, this window has been inserted into the VNC data stream so that it is effectively laid over the existing video. These menus allow you to control the many features of the **Digital KVM via IP** without using the web interface or a custom client.

Welcome Window

When you initially connect to the system, a window similar to the above one will be shown.

This tells you which system you are controlling, what encryption algorithm was used and what key strength is currently in effect. Click anywhere inside the window to clear it, or wait ten seconds.

C. How to Use the Bribar

Along the bottom of the VNC screen is a dark blue bar with various buttons. We call this feature “the bribar”. Its purpose is to show a number of critical status values and to provide shortcuts to commonly used features.
Here is a snapshot of what it may look like. There will be slight differences based on optional features and system configuration. Starting from the left side of the Bribar, each feature and its function is outlined below.

Bandwidth: Indicates current average bandwidth coming out of the **Digital KVM via IP**. The second number measures round trip time (RTT) of the connection when it was first established.

Resync: Re-aligns the remote and local mouse points so they are on top of each other.

Redraw: Redraws the entire screen contents; occurs immediately.

Video Adjust: Adjusting the video phase automatically.

PS/2 Reset: Resets the PS/2 keyboard and mouse emulation. It's very useful to recover failed mouse and/or keyboard connections in PS/2 mode.

÷4, **÷8**: Switches to thumbnail mode, at indicated size.

Ctrl-Alt-Del: Sends this key sequence to the host. It works immediately.

Alt-F4: Sends the key sequence to host (closes windows).

KVM: Calls up the KVM menu, refers to Chapter 4 for more informaton.

1~8, A~H: Select specific port simply by one click on the number.

Menu: Shows the main menu, refers to "Chapter 5, section D: How to Use the Main Menu" for more information.

Video: Shows the video-tuning menu where the picture quality can be adjusted, refers to "Chapter 5, section F: How to Use the Video Tuning Menu" for more information.

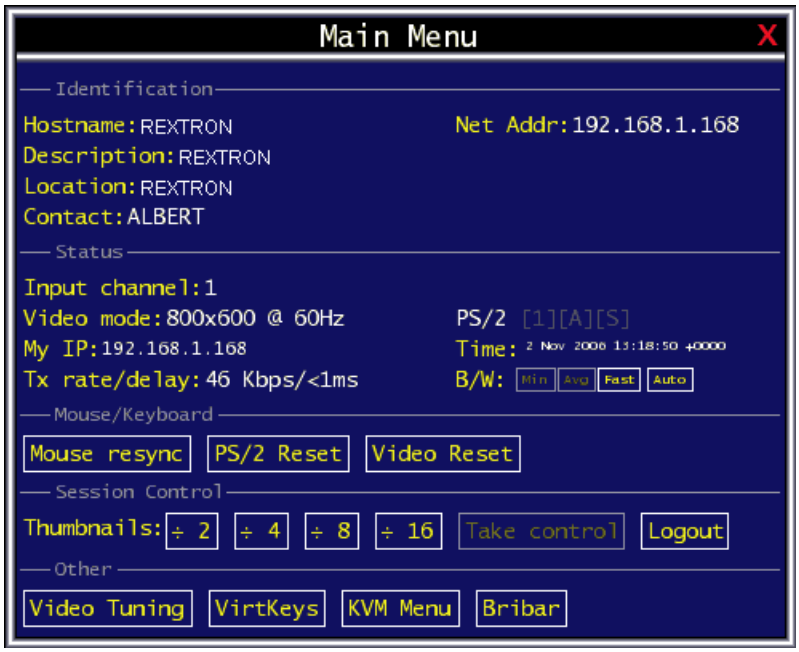
Keys: Shows the VirtKeys menu, which allows you to simulate pressing special keys such as the Windows key or complex multi-key sequences, refers to "Chapter 5, section E: How to Use the Virtkeys Menu" for more information.

Auto Bandwidth: Allows the user to select the proper bandwidth corresponds to the network environment. Generally speaking, it's recommended to select "Max" for the LAN users and "Min" for the WAN users.

PS/2: This area will show PS/2 (as in this example) to indicate if keyboard and mouse are PS/2 signals. If Autosync appears beneath this indicator, the mouse pointers on the local mouse and the VNC session will be synchronized automatically.
[1][A][S]: These flags show the state of the keyboard lights, NumLock, ShiftLock and ScrollLock respectively.
Other items: If the server's screen is larger than 1024x768, additional buttons will be shown to the right of the above listed items. These are all keyboard shortcuts and are duplicated in the Keys menu.

D. How to Use the Main Menu

To access the main menu, press ***F7*** twice quickly. You must press the key twice within one second. If you press it once or too slowly, then the ***F7*** key(s) are sent to the host, just like any other key. This is the only way to get into the menu system, if the Bribar is disabled. Here is the main menu for a typical system:



The main menu window may be moved by clicking and dragging on the title bar. It can be closed by pressing Escape, or by clicking on the red X in the top right corner.

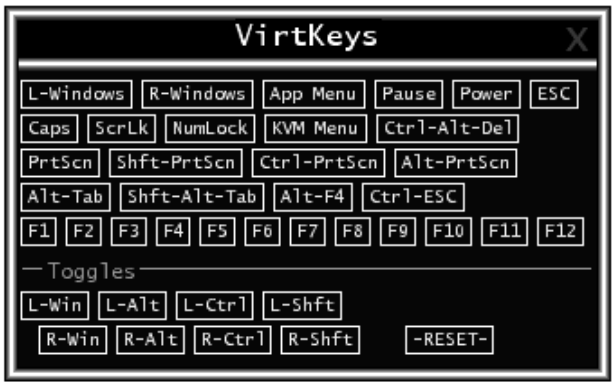
Here is a guide outlining various fields from the Main Menu. Most of the functions operate immediately. Other functions require a response to a confirmation prompt first before performing the requested function.

Identification: Fixed text label that is defined by the user in the Web interface. This does not affect the operation of the system and is intended to assist with administration.
Status: Current status of the attached system and the status of the module.
B/W Min/Avg/Max/Auto: Bandwidth control. The white button is the mode the system is currently operating. If you choose Min/Avg/Max then you will override the default, Auto. As the automatic mode measures actual network performance, you may see the current mode switch from Min up to Avg or Max. The different modes indicate more time spent on compression versus more bandwidth. There is no visual difference between the modes, but there can be a noticeable difference in speed and smoothness.
Mouse Resync: Resynchronizes the mouse pointer so that the local and remote mouse pointers are on top of each other.
PS/2 Reset: Resets the PS/2 emulation going to the host and to the attached PS/2 devices. This can be used if the mouse stops responding or the PS/2 keyboard isn't working.

Take Control: When multiple users are connected to the same system, use this button to take control away from another user. Only one user may control the keyboard and mouse at any time. All users see the same picture.
Thumbnails: Switch to smaller thumbnail size screen images (click anywhere on thumbnail to restore it). Each button corresponds to a different sized image, from half size to one-sixteenth.
Logout: End the VNC login session and disconnect.
Video Tuning: Sub-menu with video adjustments, to be used when automatic picture adjustment does not provide a good quality picture (see section below).
VirtKeys: Virtual keyboard provides a menu with special keys that are often hard to generate but needed by the remote system. The most common key sequence is the ***Ctrl*** – ***Alt*** – ***Del*** (see section below).
KVM Menu: Generates the key sequence used to access the on-screen menu for a enterprise-class KVM switch. When these conventional KVM switches are combined with the **Digital KVM via IP**, this key makes accessing their built-in menu easier, especially from the Java client. This button will only be shown when an external KVM has been enabled via the web interface.
Bribar: Closes or reopens the Bribar window along the bottom of the screen.

E. How to Use the VirtKeys Menu

This is a snapshot of the Virtual Keys window:



Clicking any button in the top half of the window simulates pressing and releasing the indicated key. In the bottom area of the screen, clicking will simulate the indicated Meta key being pressed. You may then click in the top part to send another key and release the Meta key at the same time. Alternatively, you may move the mouse outside this window, press the regular key, and then choose -RESET- to release all depressed keys.

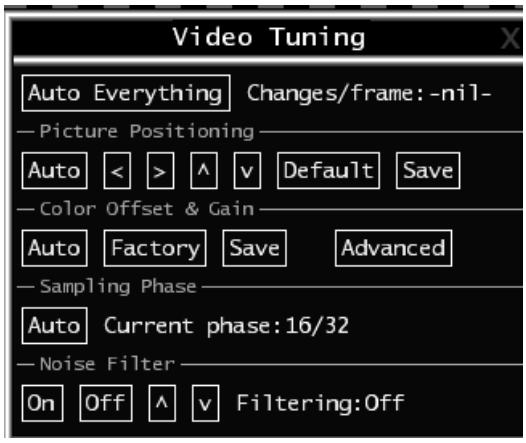
The VirtKeys menu can be left open while using the host system. You can then click the required button at the suitable time, and still interact with the host in a normal fashion.

Examples:

- ***Ctrl***–***Alt***–***F4***: Use L-***Ctrl*** then L-***Alt*** in the Toggles area. Then click ***F4***.
- **To bring up the Start menu under Windows**: Click the L-Windows button at the top left of the above window.

F. How to Use the Video Tuning Menu

This menu is used to fine-tune the video picture.



Auto Everything: use this button to automatically fine-tune all three adjustments. If the test pattern for Color Offset calibration is not present on the screen, then the Color Offset adjustment is skipped.

Changes/frame: it indicates the number of 16x16 blocks of video that are being sent, on average, for every frame of video. With a static image being displayed by the server, this number will be zero (shown as -nil-). Moving the mouse, for example, will cause the number to jump to about 2 or 3. You may use this number to judge the picture quality as you adjust the controls on this menu.

Picture Positioning: it affects the image position on your screen. If you see a black line on either side of your screen, or at the top or bottom, you can use the arrow buttons to shift the image in that direction. Pressing Auto does the same thing for you automatically. Use Save to save the changes you have made manually. Since this adjustment depends on the video mode, separate values are stored for each video mode.

Color Offset: it is a fine tuning adjustment that requires the use of a test pattern. There is a copy of the test pattern available on the Help! menu of the integrated web server. You must arrange for that image to be shown on the host computer(s). Do not allow scaling, cropping or any other changes to that image. Press the Auto button and the system will calibrate color for the best possible picture in approximately one minute. If the system cannot find the test pattern on the screen, it will say so. Check that the pattern isn't scaled or covered up. It's important to do this operation in 24-bit or 32-bit color video mode (i.e. true color). Although the algorithm may work in 16-bit or 8-bit color video modes, the results will not be optimum and usually it won't be able to recognize the test pattern.

Advanced: press this button will open the Advanced Video Tuning menu. While the vast majority of users will not need to adjust these settings, it offers a high-degree of control of the video settings of your VNC sessions.

Sampling Phase: it does not normally need to be used since our system tunes the sampling phase whenever the video mode changes. This button does not require a test pattern, but will perform optimally when used with our standard test pattern. For your reference, the sampling phase number is shown to the right of the Filtering button.

Noise Filter: it controls the advanced video filtering of our system. Unlike other filtering algorithms, our noise filter will only remove noise. It does not degrade the signal quality or readability of small text. You may turn it on and off using the indicated button, or set it to other values using the arrows. Higher numbers cause more filtering and may cause artifacts when moving windows. *The most common visual artifact is a vertical line dropping when moving windows horizontally.* You may use the Redraw button to correct these, or use a lower filter number. At minimum, these values must be greater than two.

Appendix A Troubleshooting

If you are experiencing trouble with your devices, first make sure that all cables are connected to their proper ports and are firmly seated.

How to bring up the IP-OSD menu?
Please use your paperclip or pen to press the "IP SETUP" button once to bring up the IP-OSD menu.

How to reset everything back to the factory default values?
Please use your paperclip or pen to press the "RESET" button **AND HOLD** around 8 seconds, the IP-OSD menu will automatically come up and show "All settings cleared" in red texts, and then all of the factory default values will be restored automatically.

I can't connect to the Digital KVM via IP.
Step 1. Check if the network connection is working (ping the IP address of **Digital KVM via IP**). If not, check network hardware. Is **Digital KVM via IP** powered on? Check if the IP address of **Digital KVM via IP** and all other IP related settings are correct. Also verify that all the IP infrastructure of your LAN, like routers are correctly configured. Without a ping functioning, **Digital KVM via IP** can't work. If it still can't connect to the **Digital KVM via IP**, go on the next step.
Step 2. Refer to **Quick Start Guide,** choosing the first way: **Using the IP-OSD step-by-step menu**

I can't login via SSL.
Was the correct user and password given? The default username and password as shipped from the factory is username **admin** with a password of **admin**. Configure your browser to accept cookies. The user name and password are case sensitive, check the status of the ***Caps Lock*** on your keyboard. If you see a warning about "identity of host cannot be verified", and a question about saving the host's fingerprint, this is normal for the first time you connect to any machine running SSL. You should answer "yes" so that your SSL client saves the public key of this host and doesn't re-issue this warning.

Forgotten the master password.
Reset the master password. Please refer to **Quick Start Guide,** choosing the second way**: Using the HyperTerminal via Serial Port.** Use the **S** command, and type a new password. The old password is not required for this procedure. **And, please remember to type "W" after you made any change.**

The mouse on the remote site does not work or is not synchronized.
a. Make sure there is only one mouse driver installed in each computer.
b. Set the mouse acceleration to 'None' in the host mouse driver properties.
c. Windows XP has a setting called 'Enhance pointer precision'. This should be disabled for correct mouse synchronization.

Remote mouse and local mouse don't line up.
Use the "mouse resync" command in the main menu or press the "Resync" button on the Bribar. If the mouse pointers still don't line up, verify that mouse acceleration has been disabled.
NOTE: The Windows login screen does not accept the "mouse acceleration" option, and always has the mouse accelerated regardless of your configuration. Therefore, on this screen it is best to avoid using the mouse.

After "Resync", the mouse on the remote site is synchronized, but there is small constant offset between remote and local mouse cursors.
This is a video position error. Normally a slight video positioning error is perceived as a mouse sync issue. A video positioning error is visible as a black line along the top or bottom (and right or left) edges of the remote screen. On the "Video Tuning" menu (please refers to Chapter 5, section F: How to Use the Video Tuning Menu) use the arrows under "Picture Positioning" to move the screen until the two pointers exactly line up. ***Remember to save your position changes!***

Monitor works, but keyboard and mouse do not.

Make sure you haven't swapped the keyboard and mouse cables

VGA image is not clear.
You may be using poor quality VGA cables. Make sure you are using UL-2919 rated, double-shielded VGA cables.

The quality of video is bad or the picture is grainy.
a. Use the brightness and contrast settings.
b. Use the auto adjustment feature to correct a flickering video.
c. Read and use the manual section "Chapter 5, section F: How to Use the Video Tuning Menu".
d. Also, try the "Auto everything" button on the "Video Tuning" menu.
e. Display the test pattern on the host and use "Auto Everything".
f. Try a lower refresh rate (60Hz is best)
g. Enable the noise filter and set to higher value.
h. Use lower resolution if possible (1024x768)
i. Reduce number of colors (8-bit or 16-bit color instead of 24/32).
j. Use a better quality video card.

No KVM-OSD screen or screen image.
You may have selected a power-off computer. Use the pushbuttons or to select a computer that is turned on.

There is a keyboard error on boot.
You may have a loose keyboard connection. Make sure your keyboard cables are well-seated.

The letters on the TFT LCD display are blurry or have shadows.
You may have improper resolution settings. Under the Control Panel, set the VGA output of your computers to match the highest resolution of the LCD monitor with Large Font selected.

Master/Slave does not work or there is a double KVM-OSD.
Make sure that the slave's Console port is connected to one of the Master's PC ports.
Perform a KVM Reset. Make sure that you have removed all power sources from the Slave unit before connecting it to the Master switch.

KVM-OSD menu is not in the proper position.
The KVM-OSD menu has a fixed resolution and its size varies depending on the monitor. Use F4 More/ Position (from the KVM-OSD menu) to move it to a different location.

The Up and Down arrows don't work in manual scan mode.
Make sure more than one computer is turned on. Manual Scan only works with powered computers. Check the Scan Type (from the KVM-OSD menu) and make sure you have selected the proper computers.

Auto Scan does not work.
Make sure more than one computer is turned on. Auto Scan only works with powered on computers. Check the Scan Type (from the KVM-OSD menu) and make sure you have selected the proper computers. Press the Left Control key twice or press any front pushbutton to abort the Auto Scan.

Cannot select a computer connected to a Slave.
Make sure that the Slave's Console port is connected to one of the Master's PC ports. Only ports **PC 1** to **PC 8** can be connected to Slaves, even if the Master switch has 16 PC ports.

Keyboard strokes are shifted.
Press both ***Shift*** keys.

Certificate warning shown while connecting via HTTPS.
It is normal for a warning dialog to be shown when connecting via HTTPS. The SSL certificate we use is created when the unit is first produced. It does not contain the correct hostname (subject name) because you can change the hostname as required. Also, it is not signed by a recognized certificate authority (CA) but is signed by our own signing authority. For more details, refers to “Appendix F: About Security Certificate Warnings”.

Windows XP doesn't awake from standby mode.
This is possibly a Windows XP problem. Try not to move the mouse while XP goes into standby mode.

The terminal connection to Digital KVM via IP for initial configuration cannot be established.
Check that the Null Modem cable connected to DTE Serial Port on the **Digital KVM via IP** and terminal software is set to the following line parameters:
Connection speed: 115200 bps
No. of bits: 8
Parity: None
Stop bits: 1
Flow Control: None
Connect computer to the **Digital KVM via IP** and power this computer on. Power on the **Digital KVM via IP** while pressing the ESC key on the keyboard connected to it. This will switch the DTE Serial Port to Configuration Login setting even if it was set to Pass-through or Modem.
Also, Windows HyperTerminal has a bug: if you change baud rates while connected, the screen is updated but the hardware is still at old baud rate; hang up and reconnect (using icons at top of screen) to make new settings take effect.

If my network has a firewall, what setting do I use on the IP Extender to open a port into the network?
You shouldn't change any settings in the **Digital KVM via IP**, but you should open port 22 for both outbound and inbound connections in your firewall.
Port 22 only needs to be opened for inbound connections. You must use SSH tunnel to connect to machine; tunnel to port 192.168.1.123:5900 for VNC protocol, and 192.168.123.1:80 for HTTP (web) control.

OR, instead of SSH client, open ports 443 and 15900 (inbound) for HTTPS and encrypted VNC protocol. Then click always on the "encrypted" link. This is easier because you don't need to setup SSH tunnels.

Appendix B Specifications

Maximum supported video mode	1600x1200 @ 85Hz
Standard video modes supported	640x400 @ 85Hz 720x400 @ 85Hz 640x480 @ 60Hz 640x480 @ 72Hz 640x480 @ 75Hz 640x480 @ 85Hz 800x600 @ 56Hz 800x600 @ 60Hz 800x600 @ 72Hz 800x600 @ 75Hz 800x600 @ 85Hz 1024x768 @ 60Hz 1024x768 @ 70Hz 1024x768 @ 75Hz 1024x768 @ 85Hz 1152x864 @ 75Hz 1280x960 @ 60Hz 1280x960 @ 85Hz 1280x1024 @ 60Hz 1280x1024 @ 75Hz 1280x1024 @ 85Hz 1600x1200 @ 60Hz 1600x1200 @ 65Hz 1600x1200 @ 70Hz 1600x1200 @ 75Hz 1600x1200 @ 85Hz
Color Depth	**8 BITS / 12 BITS / 16 BITS Selectable**
Maximum power consumption	18 watts
Input Connectors	Video In (for local console) PS/2 Keyboard (for local console) PS/2 Mouse (for local console) LAN RJ-45 Serial Supervisor (RJ14) DB9 RS-232 Male (DTE) DC in **MNIP01 :** 1 x HDB15 (female) Integrated KVM Cable Input **UNIP/MNIP04:** 4 x HDB15 (female) Integrated KVM Cable Input **UNIP/MNIP08:** 8 x HDB15 (female) Integrated KVM Cable Input **UNIP/MNIP16:** 16 x HDB15 (female) Integrated KVM Cable Input **WMM/WUM001:** 1 x HDB15 (female) Integrated KVM Cable Input **WMM/WUM108D:** 8 x HDB15 (female) Integrated KVM Cable Input **WMM/WUM116D:** 16 x HDB15 (female) Integrated KVM Cable Input
Dimensions W x H x D (mm)	**MNIP01:** 186 x 43 x 220 **UNIP/MNIP04:** 186 x 43 x 220 **UNIP/MNIP08:** 404 x 43 x 220 **UNIP/MNIP16:** 404 x 43 x 220 **WMM/WUM001:** 404 x 43 x 220 **WMM/WUM108D:** 404 x 43 x 220 **WMM/WUM116D:** 404 x 43 x 220
Reset button	**1. power reset (press once)** **2. reset everything back to the defaults (press and hold**

	around 8 seconds)
IP SETUP button	**Press once to bring up the IP-OSD, helping the user the step-by-step initial setup very easily without studying the user's manual**
Regulatory Certifications	FCC Class A, CE, **VCCI**
RoHS Compliant	**Yes**

Appendix C Supported Protocols

Service	Description	Benefits
SSH	Secure Shell	May be used to securely “tunnel” VNC and HTTP protocols.
HTTP	Web redirector (to HTTPS)	Convenience server to redirect all web traffic to encrypted port. Clear-text HTTP is not supported.
SNMP	SNMP Agent (UDP)	Allows integration with existing SNMP network management systems.
HTTPS	SSLTLS Encrypted web control	Secure control and management of the device and attached system. Screen snapshots may be downloaded. Integrated Java VNC client (with or without encryption) allows control from any Java-enabled browser. Password protected.
VNC	VNC/RFB Protocol Server	Standardized real-time KVM network protocol. Compatible with existing VNC client software.
VNCS	SSL-tunneled VNC	VNC protocol tunneled via SSLTLS encryption. For secure real-time control of the server over public networks.
DHCP Dynamic IP Setup Config		Eases network setup by fetching IP address and other network settings from a centralized server.
RADIUS Cen tralized authentication		Allows integration with existing RADIUS servers, so that user management can be centralized. Supports challenge-response authentication using hardware tokens (like SecurID) and conventional passwords.
SYSLOG	System event logging to another system	MIT-LCS UDP protocol. Must be configured via DHCP option.
DNS	Domain Name Service	Converts text name into IP Address Only used in the URL specification needed to emulate a CD-ROM. Use is optional.

Appendix D Warranty Information

This product is backed by a one-year warranty. In addition **Rextron** warrants its products against defects in materials and workmanship for the periods noted, following the initial date of purchase. During this period, the products may be returned for repair, or replacement with equivalent products at our discretion. The warranty covers parts and labor costs only. **Rextron** does not warrant its products from defects or damages arising from misuse, abuse, alteration, or normal wear and tear.

Limitation of Liability
In no event shall the liability to **Rextron Technology, Inc.** (or its officers, directors, employees or agents) for any damages (whether direct or indirect, special, punitive incidental, consequential, or otherwise), loss of profits, loss of business, or any pecuniary loss, arising out of related to the use of the product exceed the actual price paid for the product. Some states do not allow the exclusion or limitation of incidental or consequential damages. If such laws apply, the limitations or exclusions contained in this statement may not apply to you.

NOTE: The associated software contains encryption technology subject to the U.S. Export Administration Regulations and other U.S. law, and may not be exported or re-exported to certain countries or to persons or entities prohibited from receiving U.S. exports (including Denied Parties, entities on the Bureau of Export Administration Entity List, and Specially Designated Nationals). For more information on the U.S. Export Administration Regulations (EAR), 15 C.F.R. Parts 730-774, and the Bureau of Export Administration (BXA), see the BXA homepage at **http://www.bxa.doc.gov**

Appendix E Regulatory Compliance Statements

This device complies with part 15 of the FCC Rules for a class A digital device and also with European standards EN55022. Operation is subject to the following conditions: (1) this device may not cause harmful interference; and (2) this device must accept any interference received, including interference that may cause undesired operation.

Appendix F About Security Certificate Warnings

What is a security certificate?
Sites that employ secure TCP/IP (Internet) connections include a certificate that confirms that users are connecting to a legitimate site and are not being redirected without their knowledge. Certificates are issued by trusted third parties called Certificate Authorities (CAs) and contain essential details about a site that must match the information supplied to your Web browser.

Why do I receive a warning when I access the login screen on the Digital KVM via IP?
As it redirects you to a secure (SSL) session by default, the login screen may generate a warning from your Web browser or the VNC Java client for two different reasons. First, the CA that has issued the certificate on **Rextron**'s behalf may not yet be recognized as a trusted source by the computer you are using to access the **Digital KVM via IP**. Second, since the unit could be configured in a number different ways, it is impossible to supply a generic certificate that will match your exact network settings.

Is my data safe?
Yes. The security certificate does not affect encryption effectiveness in any way, nor does it make the **Digital KVM via IP** any more vulnerable to outside attacks.

Can I prevent the warning from occurring?
Yes. You have two options that may prevent the warning from occurring. First, if the Web browser you are using offers the option to ignore the warning for future visits, the browser will no longer generate a warning if that option is selected. Second, if you install the certificate from the KVM onto the remote computer (see below) and if the unit is configured with a domain name ending in .com, .net, .org, .gov, .edu, .us, .ca, .uk, .jp, or .tw (i.e. **remotecontrol.mydomain.net**) then the warning should no longer occur.

Installing the new certificate…
The following instructions detail how to install the certificate from the **Digital KVM via IP** onto your local computer (in this case, running Windows XP and Internet Explorer).

1. Open your Web browser and go to the **Digital KVM via IP** login screen. Click the update security certificate link.
2. When prompted, choose **Open**.
3. A Window will appear that offers information about the certificate. Click **Install Certificate**.
4. The **Certificate Import Wizard** will appear. Select **Automatically select the certificate store…** (default) and click **Next**. When the next window appears, click **Finish**.
5. A confirmation dialog will appear asking you if you wish to install the certificate. Click **Yes**.
6. A message should appear saying the import was successful. Click **OK**.

Appendix G Using Optional Serial Supervisor Module (IPMI supported) with the R-Port

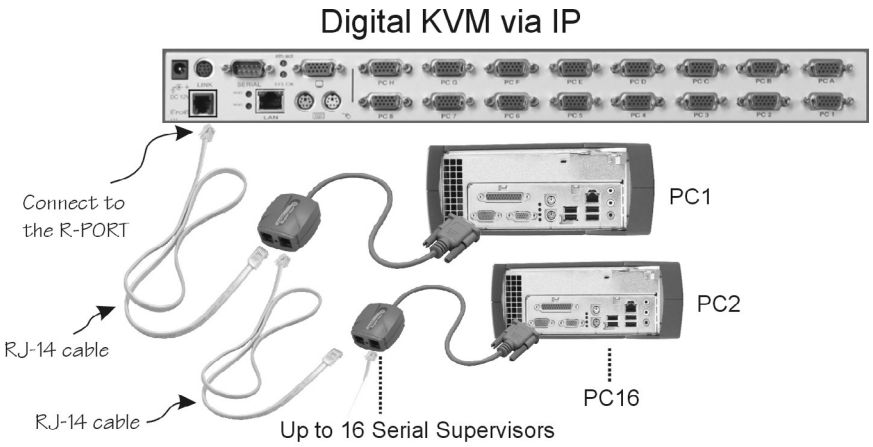
(For MNIP08/16, UNIP04/08/16, WMM001/108D/116D, WUM001/108D/116D only)

Background

The **Digital KVM via IP** offers a unique way to expand the functionality of the base product. Using R-Port on the rear panel of **Digital KVM via IP**, you can add up to 16 **Serial Supervisors** serial devices using a specialized daisy-chain technology. The **Digital KVM via IP** includes integrated control functionality that allows you to monitor and configure the devices with the RS-232 serial port using the interactive Web interface. To minimize space and infrastructure requirements, the **Serial Supervisor** uses a single cable to carry both power and the data signal. All configuration settings are stored separately in each attached **Serial Supervisor** in non-volatile memory so that they will not be lost in the event of a power outage or disconnection.

Connecting the Serial Supervisor to the Digital KVM via IP

The RJ-14 cable for link up the **Serial Supervisor** via daisy chain is similar to a phone cable. For the first computer, connect the RJ-14 cable (provided) to the R-Port on the rear panel of the **Digital KVM via IP**. Then, connect the opposite end of RJ-14 cable to the RJ-14 port of **Serial Supervisor**. There are two RJ-14 ports in the **Serial Supervisor**, please feel free to choose any one of them. Once you have added the first computer to **Digital KVM via IP** by using the **Serial Supervisor**, you can connect the second computer by using the second **Serial Supervisor**, please have your second RJ-14 cable (provided with your second **Serial Supervisor**) to link up the first **Serial Supervisor** and the second one. That's it! And, you can link up to 16 computers. The following diagram is shown the whole connection. For more specific information regarding cabling, status indicators, and how to setting, refers to the user's manual of **Serial Supervisor**.



Configuring/Viewing Serial Supervisor through the Web Interface

Once you have one or more **Serial Supervisor** connected, you will able to configure and manage them through the Web interface. You may need to modify the default settings on the **Digital KVM via IP** to match your various **Serial Supervisors**' default configuration. Consult the documentation that came with your **Serial Supervisor** to determine if you need to modify the default settings to complete the installation. To be able to configure your **Serial Supervisor**, you must be logged in as **admin**. Other users will be able to view which devices are active but cannot configure them.

Once you are logged in, choose the **Admin/Setup** option from the menu at the top of the Home screen in the Web interface. Click **External Serial consoles setup and control**. You will be presented with the **Serial Consoles Attached** menu, and a table with the following headings:

#	Name / Description	Baud (bps)	Mode	Force DCD	Console Log	Connect...

#: You can assign a value (**1 ~ 99**) to each attached serial device. This does not affect the configuration or operation of the device in any way, but is simply a means to sort this list for ease of management.

Name/Description: An identifier for the **Serial Supervisor** device. Like the number assignment, it is for ease of administration only.

Baud (bps): This is the communication speed for the device, and the setting here must match the setting on the device itself (see below). All common baud rates between 300 and 115,200 bps are supported.

Mode: Sets the character framing scheme that the **Digital KVM via IP** will use with the **Serial Supervisor** device. You can choose from the following selections:

8N1: Eight bits, no parity, one stop bit (default and most common)
7N1/701/7E1/7M1/7S1: Seven bits, (none/odd/even/mark/space) parity, one stop bit
8N1/801/8E1/8M1/8S1: Eight bits, (none/odd/even/mark/space) parity, one stop bit
8N2: Eight bits, no parity, two stop bits

Force DCD: Forces the Carrier Detect signal to be active at all times. Normally, DCD becomes active when a new user connects and is dropped when the last user disconnects (a response that is similar to many modems). When active, the device will logout and reset itself if the carrier signal is lost, increasing security. Note that this may not work with all devices and could impair proper operation in some circumstances. The default setting is off.

Console Log: Clicking this link will open a separate Web page that will display the last 200 characters committed to that device's console log. Note that existing data is overwritten automatically when the 200 character limit is reached.

(Optional, not shown) **IPMI:** This is an optional feature that requires the purchase of a software upgrade on the **Digital KVM via IP**. Refer to Appendix D for more information about purchasing and using the IPMI upgrade. This feature will not appear on the menu if the upgrade is not installed.

You can make as many changes a needed on this menu at one time before applying your changes. Once you are satisfied with the changes you have made, click **Commit changes** to apply the new settings. Click **Refresh** at any time to see an updated list of attached **Serial Supervisor** devices.

Advanced Configuration Using the Integrated SSH Shell
In most cases, configuring the **Digital KVM via IP** to the same settings as the **Serial Supervisor** devices you are connecting should allow the devices to work with a minimum amount of configuration. However, you can also change the default settings on each **Serial Supervisor** device to fit your preferences and the needs of your application.

If you click the **Connect…** button next to the device you want to configure, two new windows will appear. The smaller of the two is a login screen; the other is a SSH terminal window. Click the login window and sign in as **admin** (using the same password as the Web interface) to activate the terminal window. You will see a welcome banner similar to the following:

Baud rate: 115200 bps, 8N1
Connected to #1: (none)... (Press ***Ctrl*** + ***Shift*** + ***Space*** for menu).

You are now connected to the **Serial Supervisor** device. Commands you type will be echoed on the terminal screen. It offers a simple menu system that allows you to change its configuration settings. To access the menu press ***Ctrl*** + ***Shift*** + ***Space*** (underscore) on the keyboard to access the menu. It will be similar to the following:

```
RS-232 Menu (#1: (none), 115200 bps, 8N1)
      Q - Disconnect
      # - Send break
      H - Hangup line (drop DCD)
      E - Send Ctrl-Shift-_
      L - Low log entries (line buffer)
      1 - Show last 10 log entries
      other - Return to connection
Press key ->
```

To execute the desired command, simply press the corresponding key on the keyboard. You can also execute the command and avoid the menu by pressing the ***Ctrl*** + ***Shift*** + ***Space*** key combination quickly and pressing the letter of the command. To quit the menu, press ***Q*** on the keyboard when the menu is active.

Remote Login via SSH

You can also use a standard SSH client to access the **Serial Supervisor** options if you wish to avoid using the Java-based SSH client in the Web interface. Simply use your SSH client (several freeware packages are available for download, along with commercial applications) and connect to the IP address of the **Digital KVM via IP** using port 22 (default).

Login in to the SSH session as **admin** using the same password as the Web interface. At the command prompt type **connect x** (where **x** is the number of the **Serial Supervisor** device you wish to manage). Alternatively, you can enter the command **connect -l** to see a list of active devices.

Operating Notes

- Hardware handshaking (CTS/RTS) is required for speeds exceeding 9600 bps. It is enabled by default on the **Digital KVM via IP**, but may need to be enabled on the other end of the connection. For Unix systems, the command is:
  stty –crtscts < /dev/[serial port]
- **Serial Supervisor** devices use a simple RS-485 multidrop network running at 115,200 bps. It is possible that every **Serial Supervisor** device will not be inputting/outputting data at the same rate at all time. However, since these devices use interactive logins, it is unlikely that all channels would be busy at any one time. Hardware handshaking is used to limit the output rate of individual channels as needed.
- A maximum of four users may simultaneously login to the same device. All users may type commands at any time, and all users will see the same output. Note the following:
  - All users have equal access to all channels.
  - A maximum of 16 **Serial Supervisor** devices may be connected at any one time.

You plug-in and unplug any **Serial Supervisor** device at any time. When reconnected, it will automatically become available after a 15 second initialization period. Any log entries will be retained by the **Serial Supervisor** device while deactivated, but will not be available to users until it is re-initialized.

IPMI (Intelligent Platform Management Interface) Function

Background

To offer a more complete remote server control solution, the **DIGITAL KVM VIA IP** offers an optional power management feature that allows remote hardware restarts and the ability to power the host computer on and off. You may be able to take advantage of this feature if the host computer you are managing supports IPMI (Intelligent Platform Management Interface).

Host Computer Requirements

The host computer must support the IPMI standard version 1.5 to use this option. Most popular server motherboards now support the IPMI standard. To determine if your computer supports this IPMI, consult its documentation for more information.

IPMI is used to configure and control a device on the motherboard called the BMC (Baseboard Management Controller) using a dedicated serial port. Once the computer is configured for IPMI management, the serial port on the host computer is normally reserved by the BIOS solely for that purpose and cannot be accessed or recognized by the operating system. It is therefore unlikely that a serial port provided by an add-in card will be able to act as an IPMI port, so you must use a serial port integrated on the motherboard of the managed computer. If the computer you are managing only has a single serial port, you must add an additional port (or ports) via an add-in card if you need a serial port for other purposes (i.e. modem). Enabling IPMI support usually requires enabling options in the host computer's BIOS setup software, and the instructions will vary considerably from make to make and model to model. Normally, a password will be created by the BIOS that allows the IPMI feature to be accessed; this password is exclusive to the IPMI feature and does not correspond to a password or account in the host computer's operating system.

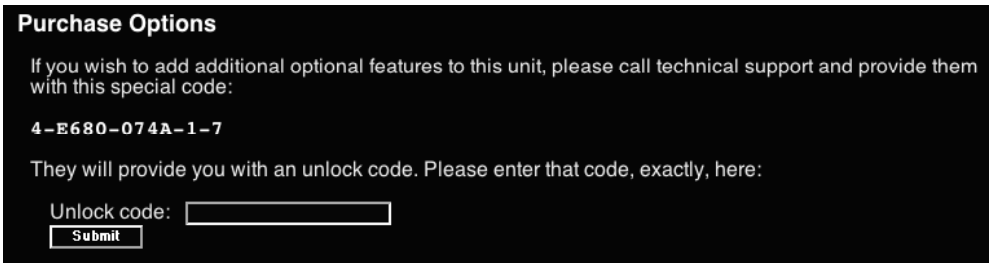
If the Host Computer Does Not Support IPMI

If the host computer you are managing with the **Digital KVM via IP** does not support IPMI, **Rextron** offers a non-IPMI solution that also works via serial port and acts as a power concentrator and a power management device: the 8 Outlet Serial Power Console and Switch. For more information about this product, visit **www.rextron.com**

Activating the IPMI Option

The **Digital KVM via IP** contains the necessary software to use IPMI. To enable this capability, you must purchase the software option from **Rextron** unless you have purchased a model with the feature pre-enabled. To verify whether the IPMI feature is enabled on your unit, login to the Web interface as **admin**, click the **Setup/Admin** button at the top of the page, and click **Firmware and flash memory management**. If **IPMI** is not listed beside **Software Options** (see above) then the IPMI option is not present and you will have to purchase the software option to use the feature.

To purchase the IPMI option, please email **Rextron** Technical Support at:
service@rextron.com


Purchase Options
If you wish to add additional optional features to this unit, please call technical support and provide them with this special code:
4-E680-074A-1-7
They will provide you with an unlock code. Please enter that code, exactly, here:
Unlock code:
Submit

Have your model and serial number on hand. When asked, supply the technician with the code listed under **Purchase Options** at the bottom of the **Firmware and flash memory management** page. Once the order is processed, the technician will provide you with an Unlock code. Enter that code in the space provided, and click **Submit**. The system will update itself to allow IPMI configuration.

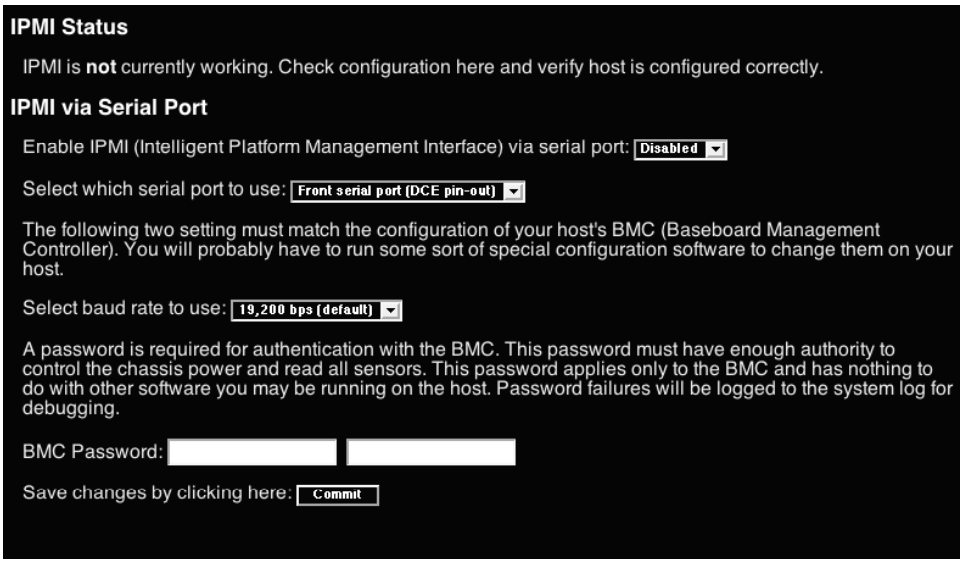
You can use either serial port on the **Digital KVM via IP** to send IPMI access; your choice will dictate the type of cable you will use to make the connection. The **DTE Serial** port on the front panel requires the use of a null modem serial cable.

Connect a female end of a serial cable to the serial port that is configured for IPMI access on the host computer. Connect the opposite end to the **DTE Serial** port of the **Digital KVM via IP**.

Configuring IPMI on the Digital KVM via IP

Once you have connected the IPMI-configured serial port to the **Digital KVM via IP** and enabled the software option, you can begin to configure IPMI settings through the Web interface.

Log in to the Web interface as **admin**. Click the **Admin/Setup** link at the top of the page and choose **IPMI/IPMB setup (Intelligent Platform Management)**.


IPMI Status
IPMI is not currently working. Check configuration here and verify host is configured correctly.
IPMI via Serial Port
Enable IPMI (Intelligent Platform Management Interface) via serial port: Disabled
Select which serial port to use: Front serial port (DCE pin-out)
The following two setting must match the configuration of your host's BMC (Baseboard Management Controller). You will probably have to run some sort of special configuration software to change them on your host.
Select baud rate to use: 19,200 bps (default)
A password is required for authentication with the BMC. This password must have enough authority to control the chassis power and read all sensors. This password applies only to the BMC and has nothing to do with other software you may be running on the host. Password failures will be logged to the system log for debugging.
BMC Password:
Save changes by clicking here: Commit

You will be presented with the **IPMI Status** menu (see above). Make the following changes to enable IPMI:

Enable IPMI (Intelligent Platform Management Interface) via serial port: select **Enabled.**
Select which serial port to use: select **Front serial port (DTE pin out)** since the **Digital KVM via IP** has **DTE serial** port only.
Select baud rate to use: select a value from the menu between **9600 bps** and **115,200 bps** based on the configuration on the host computer's IPMI settings.
BMC Password: Enter the password twice assigned to the BMC in the host computer's BIOS setup software.

NOTE: that the selected baud rate should match the host computer's setting. Problems with the BMC password (as well as any other error information) will be recorded in the **Digital KVM via IP**'s system log on the **Status** page of the Web interface. If the host computer's BIOS setup allows for multiple levels of security for the BMC, ensure the password you enter on the menu offers sufficient authority to control chassis power and monitor fan status.

Once you have made the necessary changes on this screen, click **Commit** to activate IPMI with the settings you entered. **NOTE** that clicking **Commit** will cause any active VNC sessions to fail and you will need to re-establish them.

Accessing the Status Screen

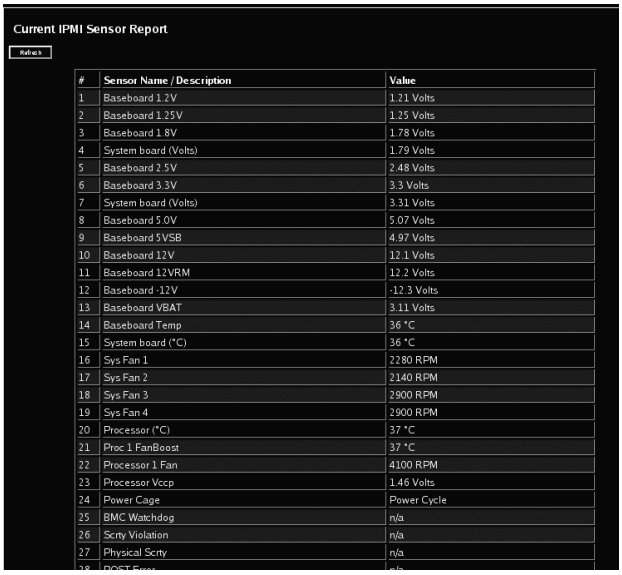
The **Digital KVM via IP** allows you to monitor the status of the host computer via IPMI using either the Web interface or the VNC client. The information you will be able to view using the status screen will depend on the model of host computer being managed. Since IPMI implementations vary widely across manufacturers, the information you are able to see on your status screen may differ from the examples. **NOTE** that the **Status** screen will not allow you to make any configuration changes and is for monitoring purposes only.

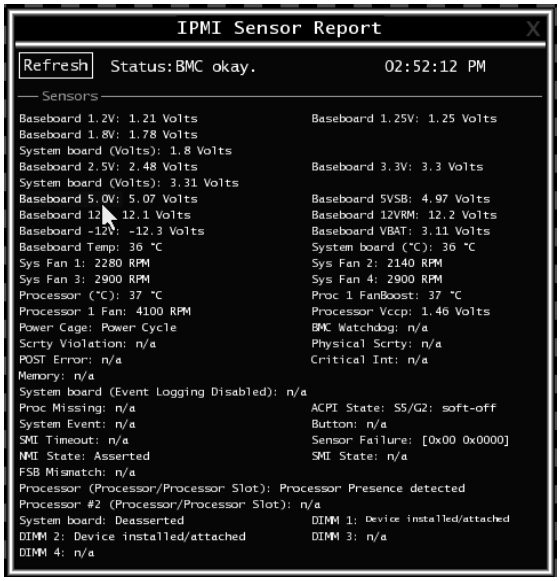
To access the **Status (IPMI Sensor Report)** screen:

From the Web interface: click **View IMPI sensor report** next to the thumbnail image on the **Home** screen

From the VNC interface: click **IMPI** from the Bribar at the bottom of the VNC window

Examples:


Current IPMI Sensor Report
Refresh
Sensor Name / Description Value
1 Baseboard 1.2V 1.21 Volts
2 Baseboard 1.25V 1.25 Volts
3 Baseboard 1.8V 1.78 Volts
4 System board (Volts) 1.79 Volts
5 Baseboard 2.5V 2.48 Volts
6 Baseboard 3.3V 3.3 Volts
7 System board (Volts) 3.31 Volts
8 Baseboard 5.0V 5.07 Volts
9 Baseboard 5VSB 4.97 Volts
10 Baseboard 12V 12.1 Volts
11 Baseboard 12VRM 12.2 Volts
12 Baseboard -12V -12.3 Volts
13 Baseboard VBAT 3.11 Volts
14 Baseboard Temp 36 °C
15 System board (°C) 36 °C
16 Sys Fan 1 2280 RPM
17 Sys Fan 2 2140 RPM
18 Sys Fan 3 2900 RPM
19 Sys Fan 4 2900 RPM
20 Processor (°C) 37 °C
21 Proc 1 FanBoost 37 °C
22 Processor 1 Fan 4100 RPM
23 Processor Vccp 1.46 Volts
24 Power Cage Power Cycle
25 BMC Watchdog n/a
26 Scrty Violation n/a
27 Physical Scrty n/a

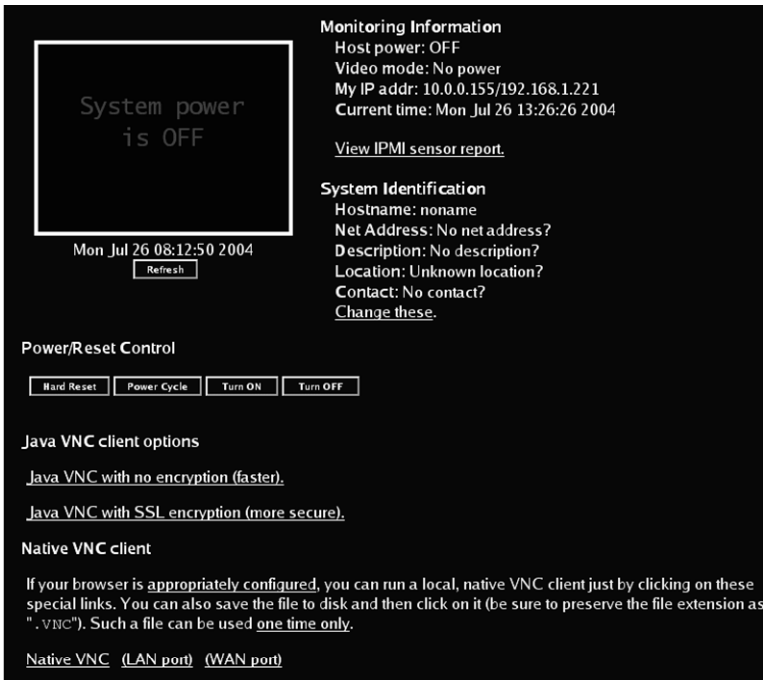


VNC Status Report

Accessing IPMI Controls

There are two ways to access power controls for the managed computer. The first is through the **Home** screen on the Web interface. The second is through the Bribar during an active VNC session.

Web


System power is OFF
Mon Jul 26 08:12:50 2004
Refresh
Monitoring Information
Host power: OFF
Video mode: No power
My IP addr: 10.0.0.155/192.168.1.221
Current time: Mon Jul 26 13:26:26 2004
View IPMI sensor report.
System Identification
Hostname: noname
Net Address: No net address?
Description: No description?
Location: Unknown location?
Contact: No contact?
Change these.
Power/Reset Control
Hard Reset
Power Cycle
Turn ON
Turn OFF
Java VNC client options
Java VNC with no encryption (faster).
Java VNC with SSL encryption (more secure).
Native VNC client
If your browser is appropriately configured, you can run a local, native VNC client just by clicking on these special links. You can also save the file to disk and then click on it (be sure to preserve the file extension as ".VNC"). Such a file can be used one time only.
Native VNC (LAN port) (WAN port)

Controls on the Home Screen (Web)

Once IPMI is enabled and functioning correctly, a set of controls will appear immediately under the thumbnail image of the host computer on the **Home** screen on the Web interface. **NOTE** that you must be logged in as **admin** to use this feature. From here, you have four options:

Hard Reset: Equivalent to pressing the RESET button on the managed computer. The computer will restart.
Power Cycle: The computer will power off, pause for a moment, and power on again automatically; equivalent to pressing the POWER button off and on again on the host computer.
Turn ON: Powers on the host computer.
Turn OFF: Powers off the host computer.

VNC

If you are inside an active VNC session and are logged in as **admin** you can use the Bribar to access IPMI features. ou have two choices from the Bribar:

Reset: Equivalent to pressing the RESET button on the managed computer. (The computer will restart.)
ON/OFF: Powers the host computer on or off depending on the current state of the host computer; equivalent to pressing the POWER button on the host computer.

NOTE: IPMI may not automatically close the host computer software safely when you issue a reset or power off command. Since these features are equivalent to pressing hardware buttons on the computer itself, the computer will respond in exactly the same way. Always shut down your operating system and application software normally before issuing an IPMI command to avoid data loss or corruption.

Appendix H Using Optional Modem Feature

- **Background**

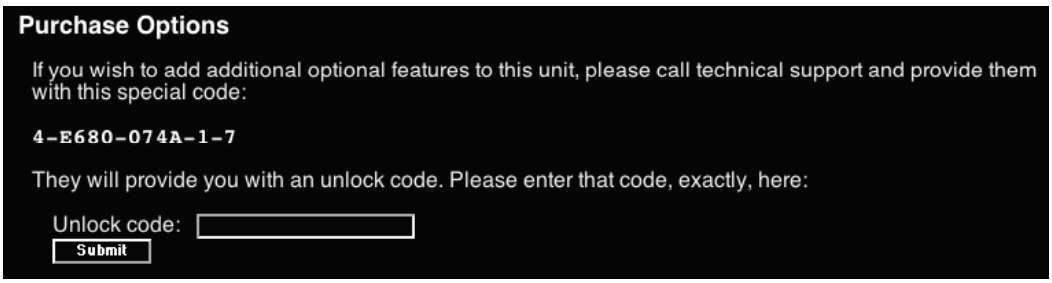
The modem option allows the Digital KVM via IP to act as an Internet connection server for increased security and flexibility in connecting with the managed computers. Unlike the TCP/IP connection used with the standard Web configuration and VNC clients, the modem creates a one-to-one connection between the **Digital KVM via IP** and the computer you are using to manage your network that is essentially private, as it bypasses the public Internet completely. Note this option requires both an external modem (most standard connection protocols are supported) and a dedicated phone line that can be connected to the modem for external access. While it is technically possible to use the modem feature through some PBX systems, this increases the complexity and reduces the performance of the connection. For clarity, the instructions presented here assume that the modem is connected to a typical POTS (plain old telephone system) line that is not routed through a phone management system or shared with other devices. If you wish to use this feature through a PBX system, it may require some experimentation and additional support from your telecom services provider, and is not supported by **Rextron**.

- **Activating the Modem Option**

A system without the modem option enabled

The **Digital KVM via IP** contains the necessary hardware to attach a modem. To enable the modem capability, you must purchase the software option from **Rextron** unless you have purchased a model with the feature pre-enabled. To verify whether the modem feature is enabled on your unit, login to the Web interface as Admin, click the Setup/Admin button at the top of the page, and click Firmware and flash memory management. If MODEM is not listed beside Software Options (see above) then the modem option is not present and you will have to purchase the software option to use the feature.

To purchase the modem option, please email **Rextron** Technical Support at
service@rextron.com


Purchase Options
If you wish to add additional optional features to this unit, please call technical support and provide them with this special code:
4-E680-074A-1-7
They will provide you with an unlock code. Please enter that code, exactly, here:
Unlock code:
Submit

Have your model and serial number on hand. When asked, supply the technician with the code listed under Purchase Options at the bottom of the Firmware and flash memory management page. Once the order is processed, the technician will provide you with an Unlock code. Enter that code in the space provided, and click Submit. The system will update itself to allow modem configuration.

- **Connecting a Modem**

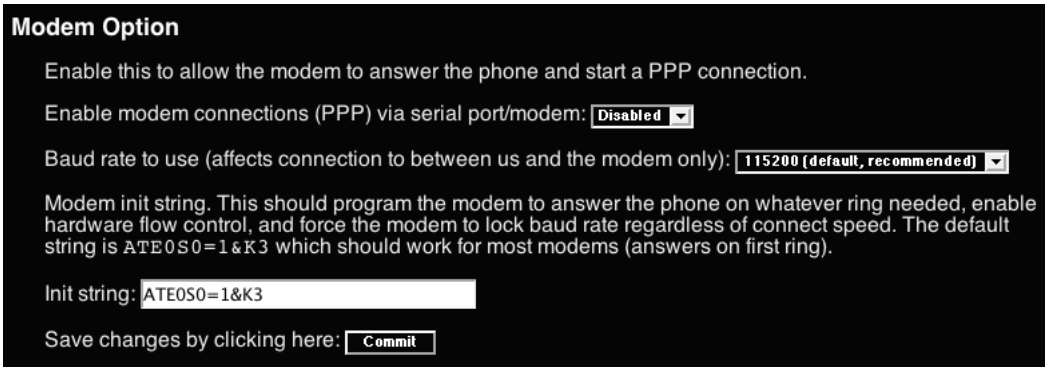
The **Digital KVM via IP** will work with virtually any Hayes-compatible modem that recognizes the standard AT command set. Some modem manufacturers offer "enterprise" grade modem products (at a premium price) that include technology to improve the stability of connections; whether this type of product would be beneficial to your application depends on whether you consider the modem connection to be mission-critical, the quality of your telecom infrastructure, and your budget for implementing this solution. The model of modem attached is essentially transparent to the **Digital KVM via IP**.

It is important to note that modems that offer "56K" (or 56,000 bps) connections often achieve connection speeds that are far lower than their maximum capabilities. Given the limitations of telecom infrastructure (many locations have yet to implement fully digital switching technology, and still rely on older analog technology for some segments), the maximum "upstream" transfer rate is limited to a maximum of 33,600 bps between two modems; the "downstream" rate is often within a similar range for a typical connection. Therefore, speeds below 56,000 bps do not indicate a problem with the modem or the but simply reflect the line conditions at the time the connection is made. The SERIAL port on the rear panel must be used for the modem connection. It requires the use of a null modem serial cable.

Place the modem near the **Digital KVM via IP** and an available telephone jack. Connect the modem to the telephone jack, data cable, and power source according to the instructions in its documentation. The opposite end of the modem's data cable should be a DB9 female serial connection. Connect that end of the cable to the SERIAL connection on the rear panel of the **Digital KVM via IP**.

Configuring a Modem Connection on the **Digital KVM via IP**
Most connections will work appropriately with the default settings on the **Digital KVM via IP** once the feature is enabled. When you entered the Unlock code to enable the feature, the **Digital KVM via IP** created a new menu option to enable configuration of this feature.

Login to the Web interface as **Admin**. Click **Admin/Setup** from the top of the page and choose **Modem (PPP) setup**.


Modem Option
Enable this to allow the modem to answer the phone and start a PPP connection.
Enable modem connections (PPP) via serial port/modem: Disabled
Baud rate to use (affects connection to between us and the modem only): 115200 (default, recommended)
Modem init string. This should program the modem to answer the phone on whatever ring needed, enable hardware flow control, and force the modem to lock baud rate regardless of connect speed. The default string is ATE0S0=1&K3 which should work for most modems (answers on first ring).
Init string: ATE0S0=1&K3
Save changes by clicking here: Commit

You will then be presented with the Modem Option menu (see above). Make the following changes to enable and configure the modem connection.

Enable modem connections (PPP) via serial port/modem: select Enabled.
Baud rate to use (affects connection between us and the modem only): select 115200.

Init string: leave as ATE0S0=1&K3 (see below).

The baud rate dictates the connection speed between the **Digital KVM via IP**'s serial port and the modem, and does not affect the connection speed between the local and remote modems, as they will negotiate their own connection speed when a connection is made. It is highly recommended that this setting be left at the default for best performance.

The init string is the command (using the standardized Hayes AT command set) that the **Digital KVM via IP** will send to the modem to activate it. The string included should work with the majority of modems and configures the following connection properties: answer incoming calls on the first ring, enable hardware flow control, and lock the connection speed. Your modem's documentation will describe other potential init strings that you can use to alter the connection properties. For instance, you could commit the settings to the modem's non-volatile memory (NVRAM) or allow the modem to adjust the connection speed for greater stability (and so on). You may wish to test the connection with the default init string first before making changes specific to your modem model or situation to simplify the troubleshooting process.

Click the Commit button to save your changes and activate the modem feature with the specified settings.

- **Configuring the Remote Connection**

This section describes how to configure a typical Windows dial-up session to access the modem connection on the **Digital KVM via IP**. The instructions here relate to a **Windows XP** configuration; other versions of Windows are similar.

Step 1. Open **My Network Places** from the desktop or the **Start** menu.
Step 2. Click **View network connections**.
Step 3. Click **Create a new connection** under **Network Tasks**.
Step 4. The **New Connection Wizard** window will open. Click **Next.**
Step 5. Select **Connect to the Internet** and click **Next**.
Step 6. Select **Set up my connection manually** and click **Next**.
Step 7. Select **Connect using a dial-up modem** and click **Next**.
Step 8. In the space provided under **ISP Name**, type an appropriate name of your choosing for the connection. Click **Next**.
Step 9. In the space provided under **Phone Number** enter the phone number for the line to which the **Digital KVM via IP**'s modem is connected. You may need to add the area code, country code, or other digits needed to access the outside line as appropriate. When finished, click **Next**.
Step 10. Make your choice from **Anyone's use** or **My use only** and click **Next**.
Step 11. Beside **User name** enter the user name of any valid user created using the Web interface of the **Digital KVM via IP**. Beside **Password** and **Confirm password** enter the password that the user you entered above uses to access the Web interface.
Step 12. This screen also includes 3 checkboxes. **Uncheck all 3 checkboxes**.
Step 13. Click **Next**.
Step 14. You may select to add a shortcut to the desktop for this connection. Click **Finish**.

You can now use this connection to access the **Digital KVM via IP** modem. Since you will still login to the unit through the Web interface after establishing a dial-up connection, the user name on the PPP connection and the user name used to access the Web interface do not have to be the same. For security purposes, you may wish to create a separate user name for dial-up access.

The unit will negotiate a PPP connection based on the settings you provided, and no additional scripting or configuration should be required under most circumstances. This is a summary of the settings for use with non-Windows operating systems, or other versions of Windows besides XP:

- PPP (Point-to-Point Protocol) must be used; no other authentication methods are supported.
- TCP/IP must be installed/enabled on the computer making the connection, and must be used for the dial-up connection.
- The connection must be configured to obtain a dynamic IP address.
- The user name/password must match a user currently configured on the **Digital KVM via IP**.
- For best performance and to simplify the troubleshooting process, firewall software should not be used with the dial-up connection.

▪ Accessing the Web Interface

Once a dial-up connection has been established, you can access the Web interface or start a VNC session using the following IP address:

https://99.99.99.99

You can now login to the Web interface (and/or VNC session) normally. Note that the remote machine (the one you dialed from) is automatically assigned the IP address 99.99.99.100 for the PPP session. This, and the IP address of the **Digital KVM via IP**, cannot be modified. The following TCP/IP port numbers are assigned for a PPP connection, regardless of the settings configured in the Web interface for the **LAN** port:

HTTPS: 443
VNC (clear-text): 5900
VNC (SSL secured): 15900
SSH: 22

▪ Performance Notes

- All images over the PPP connection will be grayscale to conserve bandwidth. If other users are connected while a PPP session is active, their screens will be in grayscale as well. When PPP in inactive, color is automatically re-enabled.
- Some areas of the screen may not be updated as frequently as others, and animations or other auto-updating areas of the screen may appear out-of-focus or “blocky” as a result. Since the area around the mouse pointer is refreshed most frequently, hold the pointer over an area to improve its clarity.
- It may be beneficial to minimize any unnecessary icons, backgrounds, or other clutter on the managed computer’s desktop to make the dial-up connection as efficient as possible.
- You will need to disable the modem feature and re-connect the serial port on the **Digital KVM via IP** to the port on a managed computer to use serial configuration.

▪ Troubleshooting Guide

The following messages will appear in the system log on the **Status** screen in the Web interface and may help to diagnose problems with the modem configuration.

Starting PPP (for auth) on port…
Modem is connecting and the PPP login process is starting.

Modem hang up. Resetting
The connection has been closed or terminated unexpectedly.

Timeout during login process. Giving up
The PPP client connecting over the modem has waited too long to complete the authentication process or supplied an invalid user name and/or password.

Modem init chat script failed
The modem did not respond to the initialization string from the **Digital KVM via IP**. You may need to change the init string or verify the cabling and modem status.

Modem init okay
The modem has responded appropriately to the init string.

Saw PPP startup from client
A PPP authentication has occurred and a session has started.

Phone line rings!
An incoming call has been detected by the modem.

Modem answers: xxxxxxxxx
The connection speed and protocol used for a connection, as reported by the modem. The exact contents of the message will vary depending on the modem make and model.

PP5-NK5400-300
Printed in Taiwan